2013 SUMMER CANDIDACY PROGRAM MATERIALS
THE CHICAGO-KENT LAW REVIEW

QUESTION

Websites collect a substantial amount of user information with technology that tracks the user's purchases, website access, posts on social media, and other internet activity. This information is added to the rest of the information available about the user on the internet, his or her "internet persona", and sold to advertisers.

In most circumstances, the website's privacy policy acknowledges this practice and equates use of the website with the user's acceptance of its privacy policy. Courts in the U.S. have validated this practice of equating use of a website with acceptance of a website's privacy policy, which has resulted in the continued collection and sale of individual information. These decisions have received substantial criticism from privacy advocates, but strong praise from advertising agencies and various other interested parties.

Using only the sources contained in this packet, write an academic article (15 pages, maximum)

(1) Analyzing court decisions regarding the legality of the current practice;
(2) Discussing whether the current practice should continue considering the benefits and harms; and
(3) Taking a stand as to what courts or the legislature should do (if anything) to change or preserve the legal status quo.

Outside research is strictly forbidden. You can analyze the statements or propositions from other sources discussed in the SCP materials. However, you cannot obtain and read those sources; neither should you cite them directly. Keep in mind that not every word of every source relates to the issue. You must determine what is relevant. No knowledge of any outside legal subject is required to respond to these questions effectively.

Although many of the jurisdictions referenced in the sources below follow their own procedural rules, assume for this exercise that all such rules are substantially similar to any Federal Rules.

Read and follow the 2013 Summer Candidacy Program Instructions, available on the CHICAGO-KENT LAW REVIEW website (www.cklawreview.com).

RESEARCH UNIVERSE

Contents

Electronic Communications Act - Definitions
§ 2510. Definitions
United States Code Annotated
Title 18. Crimes and Criminal Procedure
Effective: November 2, 2002

§ 2510. Definitions

As used in this chapter--

(1) “wire communication” means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) “oral communication” means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

(3) “State” means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(4) “intercept” means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.1

(5) “electronic, mechanical, or other device” means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than--

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal;

(6) “person” means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation;

(7) “Investigative or law enforcement officer” means any officer of the United States or of a State or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter, and any attorney authorized by law to prosecute or participate in the prosecution of such offenses;

(8) “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;
(9) “Judge of competent jurisdiction” means--
(a) a judge of a United States district court or a United States court of appeals; and
(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire, oral, or electronic communications;
(10) “communication common carrier” has the meaning given that term in section 3 of the Communications Act of 1934;
(11) “aggrieved person” means a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed;
(12) “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--
(A) any wire or oral communication;
(B) any communication made through a tone-only paging device;
(C) any communication from a tracking device (as defined in section 3117 of this title); or
(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;
(13) “user” means any person or entity who--
(A) uses an electronic communication service; and
(B) is duly authorized by the provider of such service to engage in such use;
(14) “electronic communications system” means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;
(15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications;
(16) “readily accessible to the general public” means, with respect to a radio communication, that such communication is not--
(A) scrambled or encrypted;
(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;
(C) carried on a subcarrier or other signal subsidiary to a radio transmission;
(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or
(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to

broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means--

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) "foreign intelligence information", for purposes of section 2517(6) of this title, means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

i. actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

ii. sabotage or international terrorism by a foreign power or an agent of a foreign power; or

iii. clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

i. the national defense or the security of the United States; or

ii. the conduct of the foreign affairs of the United States;

(20) "protected computer" has the meaning set forth in section 1030; and

(21) "computer trespasser"--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

Computer Fraud and Abuse Act
§ 1030. Fraud and related activity in connection with computers
United States Code Annotated
Title 18. Crimes and Criminal Procedure
Effective: September 26, 2008

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

A. information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

B. information from any department or agency of the United States; or

C. information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

A. knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

B. intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

C. intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

A. such trafficking affects interstate or foreign commerce; or

B. such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--

A. threat to cause damage to a protected computer;

B. threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

C. demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

…

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

…

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

a. the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

…

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) **…**

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may

be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

Federal Wiretap Act / Electronic Communications Act
§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited
United States Code Annotated
Title 18. Crimes and Criminal Procedure
Effective: July 10, 2008

(1) Except as otherwise specifically provided in this chapter any person who--
  (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
  (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when--
    i. such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
    ii. such device transmits communications by radio, or interferes with the transmission of such communication; or
    iii. such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
    iv. such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
    v. such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;
  (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
  (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
  (e) (i) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b)-(c), 2511(2)(e), 2516, and 2518 of this chapter, (ii) knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation, (iii) having obtained or received the information in connection with a criminal investigation, and (iv) with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation,

  shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2) **…**

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

…

Stored Communications Act
§ 2701. Unlawful access to stored communications
United States Code Annotated
Title 18. Crimes and Criminal Procedure
Effective Nov. 25, 2002

(a) **Offense.**--Except as provided in subsection (c) of this section whoever--
- **(1)** intentionally accesses without authorization a facility through which an electronic communication service is provided; or
- **(2)** intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) **Punishment.**--The punishment for an offense under subsection (a) of this section is--
- **(1)** if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State--
  - **(A)** a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and
  - **(B)** a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and
- **(2)** in any other case--
  - **(A)** a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and
  - **(B)** a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) **Exceptions.**--Subsection (a) of this section does not apply with respect to conduct authorized—
- **(1)** by the person or entity providing a wire or electronic communications service;
- **(2)** by a user of that service with respect to a communication of or intended for that user; or
- **(3)** in section 2703, 2704 or 2518 of this title.

Illinois Personal Information Protection Act - Definitions
530/5. Definitions
West's Smith-Hurd
Illinois Compiled Statutes Annotated
Chapter 815. Business Transactions
Effective: January 1, 2012

§ 5. Definitions. In this Act:

“Data Collector” may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

“Breach of the security of the system data” or “breach” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. “Breach of the security of the system data” does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

“Personal information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(1) Social Security number.
(2) Driver's license number or State identification card number.
(3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

“Personal information” does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

Illinois Personal Information Protection Act
530/10. Notice of Breach
West's Smith-Hurd
Illinois Compiled Statutes Annotated
Chapter 815. Business Transactions
Effective: January 1, 2012

§ 10. Notice of Breach.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system. The disclosure notification to an Illinois resident shall include, but need not be limited to, (i) the toll-free numbers and addresses for consumer reporting agencies, (ii) the toll-free number, address, and website address for the Federal Trade Commission, and (iii) a statement that the individual can obtain information from these sources about fraud alerts and security freezes. The notification shall not, however, include information concerning the number of Illinois residents affected by the breach.

(b) Any data collector that maintains or stores, but does not own or license,computerized data that includes personal information that the data collector does not own or license shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. In addition to providing such notification to the owner or licensee, the data collector shall cooperate with the owner or licensee in matters relating to the breach. That cooperation shall include, but need not be limited to, (i) informing the owner or licensee of the breach, including giving notice of the date or approximate date of the breach and the nature of the breach, and (ii) informing the owner or licensee of any steps the data collector has taken or plans to take relating to the breach. The data collector's cooperation shall not, however, be deemed to require either the disclosure of confidential business information or trade secrets or the notification of an Illinois resident who may have been affected by the breach.

(c) (b-5) The notification to an Illinois resident required by subsection (a) of this Section may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the data collector with a written request for the delay. However, the data collector must notify the Illinois resident as soon as notification will no longer interfere with the investigation.

(d) For purposes of this Section, notice to consumers may be provided by one of the following methods:
    (1) written notice;
    (2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or
    (3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be

notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media.

(e) Notwithstanding any other subsection in this Section, a data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

Restatement (Second) of Torts § 652B (1977)
Restatement of the Law — Torts
Restatement (Second) of Torts
Current through August 2012

§ 652B. Intrusion Upon Seclusion

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652C (1977)
Restatement of the Law — Torts
Restatement (Second) of Torts
Current through August 2012

§ 652C. Appropriation Of Name Or Likeness

One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.

Restatement (Second) of Torts § 652D (1977)
Restatement of the Law — Torts
Restatement (Second) of Torts
Current through August 2012

§ 652D. Publicity Given To Private Life

One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that

(a) would be highly offensive to a reasonable person, and
(b) is not of legitimate concern to the public.

Restatement (Second) of Torts § 652E (1977)
Restatement of the Law — Torts
Restatement (Second) of Torts
Current through August 2012

§ 652E. Publicity Placing Person In False Light

One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if

(a) the false light in which the other was placed would be highly offensive to a reasonable person, and
(b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

Restatement (Second) of Torts § 217 (1965)
Restatement of the Law — Torts
Restatement (Second) of Torts
Current through August 2012

§ 217. Ways Of Committing Trespass To Chattel

A trespass to a chattel may be committed by intentionally
(a) dispossessing another of the chattel, or
(b) using or intermeddling with a chattel in the possession of another.

Restatement (Second) of Torts § 158 (1965)
Restatement of the Law — Torts
Restatement (Second) of Torts
Current through August 2012

§ 158. Liability For Intentional Intrusions On Land

One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally

(a) enters land in the possession of the other, or causes a thing or a third person to do so, or
(b) remains on the land, or
(c) fails to remove from the land a thing which he is under a duty to remove.

Bose v. Interclick, Inc.

2011 WL 4343517
August 17, 2011
Not Reported in F.Supp.2d
(Only the Westlaw citation is currently available.)
United States District Court,
S.D. New York.
No. 10 Civ. 9183(DAB).

Opinion

MEMORANDUM AND ORDER

DEBORAH A. BATTS, District Judge.

*1 Plaintiff Sonal Bose ("Bose"), individually and on behalf of all others similarly situated, brings suit against Defendant Interclick, Inc. ("Interclick"), an Advertising Network company, and McDonald's USA LLC, McDonald's Corp., CBS Corp., Mazda Motor Corp. of America, Inc., Microsoft Corp., and Does 1–50 (collectively, the "Advertiser Defendants") under the Computer Fraud and Abuse Act ("CFAA"), New York General Business Law Section 349, and New York State common law. All Defendants move to dismiss on the grounds that Plaintiff fails to allege cognizable injury or meet the $5,000.00 threshold to state a claim under the CFAA, and that Plaintiff's state law claims fail as a matter of law. For the reasons below, Defendants' Motions to Dismiss are GRANTED in part and DENIED in part.

I. BACKGROUND

The facts and allegations are set forth in Bose's Amended Complaint ("Am.Compl."). Bose's factual assertions are assumed true for the purposes of this motion.

Bose is a resident of the city, county, and state of New York. (Am.Compl.¶ 7.) Bose is a consumer who frequently uses the Internet. (Id. ¶ 76.)

Interclick is an "Advertising Network" company. (Id. ¶¶ 8, 24.) Interclick purchases advertisement display space from websites, and displays advertisements of interest to a computer user. (Id. ¶ 30.) Websites on the Internet frequently display third-party advertisements. (Id. 130.) These websites sell advertising display space either directly to advertisers or to Advertising Network companies like Interclick. (Id. ¶¶ 24–25.) Interclick's clients are advertising companies and agencies that pay fees to Interclick to display their advertisements on websites within Interclick's advertising network. (Id. ¶¶ 21, 24.)

Many Advertising Network companies use "browser cookies," which are text files that gather information about a computer user's internet habits. (Am.Compl.¶ 30.) Browser cookies contain unique identifiers and associate "browsing history information" with particular computers. (Id. ¶ 30.) Advertising Networks use this browsing history information to create "behavioral profiles."

When a computer user visits a web page on which the Advertising Network provides advertisements, the Advertising Network company uses a behavioral profile to select particular advertisements to display on that computer. (Id. ¶ 30.) Computer users can delete these browser cookies to prevent third parties from associating the user's browsing history information with their subsequent web activity. (Id. ¶¶ 32, 82.)

Bose, however, alleges that Interclick used "flash cookies" (or Local Shared Objects ("LSOs")) to back up browser cookies. (Am.Compl.¶ 39.) When a computer user deletes a browser cookie, the flash cookie "respawns" the browser cookie without notice to or consent of the user. (Id. ¶ 39.) The flash cookie "may be" larger than a browser cookie. (Id. ¶ 88.) In October 2010, Bose examined her computer and found a flash cookie placed there from Interclick. (Id. ¶ 77.)

*2 Bose also alleges that Interclick used "history sniffing" code invisible to the computer user. (Am.Compl.¶ 47.) This code, which contained a list of Web page hyperlinks, used the computer's browser to determine whether the computer had previously visited those hyperlinks, and transmitted the results to Interclick's servers. (Id. ¶ 47.) Interclick used data on the computer's browsing history to select particular advertisements to display on that computer. (Id. ¶ 47.)

On December 8, 2010, Bose filed suit against Interclick. A suit against the Advertiser Defendants followed on December 23, 2010, and those cases were consolidated with the filing of the First Amended Complaint on March 21, 2011. Plaintiff alleges that Interclick violated the CFAA by monitoring Plaintiff's web browsing. (Id. ¶ 1.) Bose alleges that the Defendants invaded her privacy, misappropriated personal information, and interfered with the operation of her computer. (Id. ¶ 3.) On April 18, 2011, all Defendants moved to dismiss for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6).

II. DISCUSSION

…

B. The Computer Fraud and Abuse Act

*3 The CFAA provides, in pertinent part, "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer ... shall be punished." 18 U.S.C. § 1030(a)(2)(C). Under § 1030(a)(5)(C), the CFAA also subjects to criminal liability someone who "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage."

Although the CFAA is a criminal statute, it also provides a civil remedy. Under the civil enforcement provision of the CFAA, "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief ." 18 U.S.C. § 1030(g); see also Nexans Wires S.A. v. Sark–USA, Inc., 166 Fed. App'x 559, 562 (2d Cir. Feb.13, 2006) (recognizing that a Plaintiff can only bring a civil action if the Plaintiff satisfies one of five factors set forth in § 1030(c)(4)(A)(i)1). The relevant factor in this case is whether Defendants' conduct caused "loss to 1 or more persons during any 1–year period ... aggregating at least $5,000 in value." § 1030(c)(4)(A) (i)(I).

1. Damage or Loss under the CFAA

The CFAA defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.” § 1030(e)(8). “Loss,” in turn, includes “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” § 1030(e)(11). In addition, any damage or loss must meet the $5,000.00 minimum statutory threshold specified in § 1030(c)(4)(A)(i)(I). Register.com, Inc. v. Verio, 356 F.3d 393, 439 (2d Cir.2004) (citing In re Double C lick Inc. Privacy Litiq., 154 F.Supp.2d 497, 520–23 (S.D.N.Y.2001)).

Here, Bose pleads three types of damage or loss: (1) damage due to impairment of Bose's computer and computer-related services and resources; (2) loss due to Interdict's collection of personal information from Bose; and (3) loss due to an interruption of Bose's Internet service. (Am.Compl.¶¶ 94–116.)

a. Damage to Computer–Related Resources

With regard to damage or impairment of a computer system, physical damage to a computer is not necessary to allege damage or loss. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir.2001) (noting that instances of physical damage to computers are likely to become less common while the value and cost of maintaining computer security are increasing); see also Tyco Int'l (US) Inc. v. John Does 1–3, No. 01 Civ. 3856, 2003 WL 21638205, at *1 (S.D.N.Y. July 11, 2003). Any loss incurred from “securing or remedying” a computer system after an alleged CFAA violation still constitutes loss. In re Double C lick Inc. Privacy Litig., 154 F.Supp.2d 497, 524 (S.D.N.Y.2001) (“S.Rep. No. 104–357 seems to make clear that Congress intended the term ‘loss' to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker.”). Accordingly, Courts have sustained claims where a Defendant accessed a Plaintiff's computer system in order to copy the Plaintiff's system for the Defendant's own competitor computer system. I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info., 307 F.Supp.2d 521, 525 (S.D.N.Y.2004) (finding that harm to the integrity of plaintiff's data system constitutes loss).

*4 Courts have found that losses include the costs of seeking to “identify evidence of the breach, assess any damage it may have caused, and determine whether any remedial measures were needed to rescue the network.” Univ. Sports Pub. Co. v. Playmakers Media Co., 725 F.Supp.2d 378, 388 (S.D.N.Y.2010); see also Ipreo Holdings LLC v. Thomson Reuters Corp., No. 09 CV 8099(BSJ), 2011 WL 855872, *7 (S.D.N.Y. Mar.8, 2011) (holding that a Plaintiff can meet the loss requirement through “damage assessment and/or remedial measures, even without pleading actual damage”); Kaufman v. Nest Seekers, LLC, No. 05 CV 6782(GBD), 2006 WL 2807177, at *8 (S.D.N.Y. Sept.26, 2006) (denying motion to dismiss because “costs involved in investigating the damage to [a] computer system may constitute ... loss”); see also I.M.S. Inquiry Mgmt. Sys., Ltd., 307 F.Supp.2d 521 at 526 (holding that a Plaintiff sufficiently alleged loss where Defendant's unauthorized activity “forced Plaintiff to incur costs of more than $5,000 in damage assessment and remedial measures”).

Here, Bose fails to quantify any damage that Interclick caused to her "computers, systems or data that could require economic remedy." See In re DoubleClick Inc. Privacy Litig., 154 F.Supp.2d at 521. Bose alleges that Interclick impaired the functioning and diminished the value of Bose's computer in a general fashion (See Am. Compl. ¶ 115), but fails to make any specific allegation as to the cost of repairing or investigating the alleged damage to her computer. See Fink v. Time Warner Cable, No. 08 Civ. 9628(LTS)(KNF), 2009 WL 2207920, *4 (S.D.N.Y. July 23, 2009) (dismissing a CFAA claim because Plaintiff only alleged that Defendant caused damage by "impairing the integrity or availability of data and information," which was "insufficiently factual to frame plausibly the damages element of Plaintiff's CFAA claim"); see also Czech v. Wall St. on Demand, Inc., 674 F.Supp.2d 1102, 1118 (D.Minn.2009) (holding that a Plaintiff's claim that unwanted text messages "caused the wireless devices of [Plaintiff] to slow and/or lag in operation" and "impair[ ] the availability of and interrupt[ ] the wireless-device service," was conclusory). Bose's claims therefore fail because she does not quantify the repair cost or cost associated with investigating the alleged damage.

b. Collection of Personal Information

Bose's allegations concerning "invasion of [her] privacy," "trespass," and "misappropriation of confidential data" are also not cognizable economic losses. See In re Double C lick Inc. Privacy Litig., 154 F.Supp.2d at 524 n. 33; see also S. Rep No. 101–544 (1990) (noting that the CFAA is limited to "economic damages," except for violations related to medical records).

Only economic damages or loss can be used to meet the $5,000.00 threshold. In re DoubleClick Inc. Privacy Litig., 154 F.Supp.2d at 519 (holding that computer users' demographic information were not compensable "economic damages"); see also Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd., 387 F.Supp.2d 378, 382 (S.D.N.Y.2005) (holding that lost profits from defendant's unfair competitive edge were not economic damages under the CFAA). The limit based on economic damages under the CFAA "precludes damages for death, personal injury, mental distress, and the like." Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 935 (9th Cir.2004).

*5 Here, Bose alleges loss from Interclick's collection of her personal information without her permission through flash cookies and history sniffing code. (Am.Compl.¶¶ 94–109.) Unlike in DoubleClick, where Plaintiffs could "easily and at no cost prevent [the Defendant] from collecting information by simply selecting options on their browsers or downloading an 'opt out' cookie," Bose alleges that Interclick circumvented "browser privacy controls" without her consent. (Am.Compl.¶ 79); see 154 F.Supp.2d at 521.

This Court is not persuaded by Plaintiff's attempt to distinguish DoubleClick. In LaCourt v. Specific Media, Inc., a court in the Central District of California dismissed a CFAA claim by plaintiffs who alleged that they set "privacy and security controls" on their computers to block and delete third party cookies, and that the defendant had a "Flash cookie" installed on plaintiffs' computers without notice or consent. See LaCourt v. Specific Media, Inc., No. SACV 10–1256–GW(JCGx), 2011 WL 1661532, at *1 (C.D.Cal. Apr. 28, 2011). Finding that plaintiffs had failed to allege economic injury, the court noted,

> the Complaint does not identify a single individual who was foreclosed from entering into a 'value-for-value exchange' as a result of [defendant's] alleged conduct. Furthermore, there are no facts in the [complaint] that indicate that the Plaintiffs themselves ascribed an economic value to their unspecified personal information. Finally, even assuming an opportunity to engage in a 'value-for-value exchange,' Plaintiffs do not explain how they were 'deprived' of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party.

LaCourt, 2011 WL 1661532, at *5.

The deficiencies noted by the court in LaCourt are also present here.

Furthermore, as noted by the court in DoubleClick, personal data and demographic information concerning consumers are constantly collected by marketers, mail-order catalogues and retailers. In re DoubleClick Inc. Privacy Litiq., 154 F.Supp.2d at 525. The collection of demographic information does not "constitute[ ] damage to consumers or unjust enrichment to collectors." Id. Advertising on the Internet is no different from advertising on television or in newspapers. Id. Even if Bose took steps to prevent the data collection, her injury is still insufficient to meet the statutory threshold. See LaCourt, 2011 WL 1661532, at *5 (holding that a Plaintiff's inability to delete or control cookies may constitute de minimis injury, but such injury was still insufficient to meet the $5,000.00 threshold).

The court's reasoning in DoubleClick is still persuasive, as the court concluded in LaCourt:

> While Plaintiffs attempt to distinguish DoubleClick on the ground they have alleged that they were deprived not of "mere demographic information," but "of the value of their personal data," it is not clear what they mean by this. Defendant observes that, if anything, the Plaintiffs in DoubleClick alleged that the Defendant collected much more information than Specific Media supposedly collected in this case, including "names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect."

*6 Id. (citing In re Double C lick Inc. Privacy Litig., 154 F.Supp.2d at 503).

Bose's claim that Interclick collected her personal information therefore does not constitute cognizable loss sufficient to meet the $5,000.00 statutory threshold.

c. Interruption of Service.

Bose also fails to allege specific damage or loss incurred due to alleged interruption of service, or costs incurred to remedy the alleged interruption of service. (Am.Compl.¶ 111–116.) Even if a flash cookie may reach up to 100 kilobytes in size and may occupy space on Bose's hard drive, Bose fails to demonstrate that the flash cookie caused damage, a slowdown, or a shutdown to her

computer. See Czech, 674 F.Supp.2d at 1117 (holding that damage caused by an "impairment of performance" of a cell phone occurs only when the "cumulative impact of all calls or messages at any given time exceeds the device's finite capacity so as to result in a slowdown, if not an outright 'shutdown,' of service"). Thus, Bose's claim of interruption of service is insufficient to meet the $5,000.00 statutory threshold for loss.

2. Aggregation

Bose alleges that when her claims and other class members' claims are aggregated, the $5,000.00 threshold is met. (Am.Compl.¶¶ 120, 150.)

The Second Circuit has not yet addressed whether losses can be aggregated for purposes of the CFAA before a class is certified, but it has indicated approval of DoubleClick 's thorough exploration of the CFAA. Register.com, Inc., 356 F.3d at 439–440 (noting in DoubleClick "excellent statutory construction analysis and thorough exploration of legislative history"). In DoubleClick, the court concluded that damage and loss may only be "aggregated across victims and over time" for a "single act." 154 F.Supp.2d at 523 (declining to aggregate claims that defendant placed cookies on multiple computers and noting that the CFAA defines damage in § 1030(e)(8) in the singular form, "any impairment to the integrity or availability of data, a program, a system, or information," rather than the plural form, "any impairments to the integrity or availability of data, programs, systems, or information"); see also S.Rep. No. 99–132, at 5 (1986) (explaining that loss caused by the "same act" can be aggregated to meet the $5,000.00 threshold). Plaintiff's claims that Interclick placed cookies on multiple computers could not be aggregated to reach the $5,000.00 threshold under the reasoning in DoubleClick.

Moreover, even if a plaintiff represents a class, she must still demonstrate that she herself has been personally injured. Lewis v. Casey, 518 U.S. 343, 357, 116 S.Ct. 2174, 135 L.Ed.2d 606 (1996); see also In re America Online, Inc., 168 F.Supp.2d 1359, 1374–75 (S.D.Fla.2001) (dismissing a CFAA claim even if damages can be aggregated across multiple computers because Plaintiff failed to specify individuals who suffered the loss, whether they were individuals within the class, outside the class or named representatives).
…
Accordingly, Bose's Amended Complaint must be dismissed because she failed to assert personal economic loss under the CFAA.

C. State Law Claims
…
i. New York General Business Law § 349

*8 Plaintiff alleges that Defendants' information collecting activities constitute a deceptive business act or practice under Section 349 of the New York General Business law. (Am.Compl.¶ 155.) Section 349 was originally enacted as a broad consumer protection measure. See Stutman v. Chemical Bank, 95 N.Y.2d 24, 28, 709 N.Y.S.2d 892, 731 N.E.2d 608 (N.Y.2000); N.Y. Gen. Bus. Law. § 349 (McKinney 2011). To state a claim under Section 349, a plaintiff must demonstrate three elements: "first, that the challenged act or practice was consumer-oriented; second, that it was misleading in a material way; and third, that the plaintiff suffered injury as a

result of the deceptive act." Id. at 29, 709 N.Y.S.2d 892, 731 N.E.2d 608; see also Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, 85 N.Y.2d 20, 25, 623 N.Y.S.2d 529, 647 N.E.2d 741 (N.Y.1995). The deceptive practice must be "likely to mislead a reasonable consumer acting reasonably under the circumstances." Oswego, 85 N.Y.2d at 26, 623 N.Y.S.2d 529, 647 N.E.2d 741. "The phrase deceptive acts or practices" under the statute is not the mere invention of a scheme or marketing strategy, but the actual misrepresentation or omission to a consumer." Goshen v. Mutual Life Ins. Co. of N.Y., 98 N.Y.2d 314, 325, 746 N.Y.S.2d 858, 774 N.E.2d 1190 (N.Y.2002). In addition, a plaintiff must prove "actual" injury to recover under the statute, though not necessarily pecuniary harm. Oswego, 85 N.Y.2d at 26, 623 N.Y.S.2d 529, 647 N.E.2d 741.

Plaintiff alleges that Defendant Interclick used LSOs and browser history sniffing code to circumvent consumers' ordinary browser privacy and security settings on their computers. (Am.Compl.¶ 156.) This conduct misled consumers into believing their digital information was private when in reality it was being tracked without their knowledge. (Am.Compl.¶ 157.) Plaintiff alleges that consumers were harmed in that they suffered "the loss of privacy through the exposure of the [sic] personal and private information and evasion of privacy controls on their computers." (Am.Compl.¶ 160.)

Interclick first argues that Plaintiff cannot meet the second element of a claim under Section 349 because Plaintiff has failed to allege misleading conduct on the part of Interclick. Interclick argues that as Plaintiff was unaware of Interclick's actions while they were occurring, Plaintiff could not have been misled into entering into any consumer transaction. (Interclick Mem. L., p. 18.) Interclick would thus have this Court interpose a reliance element into the Section 349 analysis. The New York Court of Appeals has specifically rejected that proposition. See Stutman, 95 N.Y.2d at 30, 709 N.Y.S.2d 892, 731 N.E.2d 608 ("Plaintiffs need not additionally allege that they would not otherwise have entered into the transaction.")

In its reply papers, Interclick modifies its argument slightly, contending that Plaintiff fails to allege any misrepresentation or omission by Interclick to Plaintiff. (Interclick Rep. Mem. L., at 8 .) Although the paradigmatic case under Section 349 involves a business making a false or misleading statement in advertising aimed at consumers, see, e.g., Waldman v. New Chapter, Inc., 714 F.Supp.2d 398, 405 (E.D.N.Y.2010), courts have allowed claims under Section 349 where misleading statements are made to third parties resulting in harm to consumers. See Securitron Magnalock Corp. v. Schnabolk, 65 F.3d 256, 264 (2d Cir.1995) (finding false statements by a competitor to a regulatory agency actionable under Section 349); Kuklachev v. Gelfman, 600 F.Supp.2d 437, 476 (E.D.N.Y.2009) ("The relevant question 'is whether the matter affects the public interest in New York, not whether the suit is brought by a consumer.' ") (quoting Securitron, 65 F.3d at 257). A claim under Section 349 need not, as Interclick argues, involve an allegation of a deceptive statement made by Interclick to Plaintiff. It need only allege that Interclick engaged in a deceptive practice that affected the consuming public. Plaintiff has alleged as much.

*9 Interclick next claims that Plaintiff has failed to allege any injury as a result of any misleading act or omission. To state a claim under Section 349, a plaintiff must allege "actual" injury, though not necessarily pecuniary injury. Stutman, 95 N.Y.2d at 29, 709 N.Y.S.2d 892, 731

N.E.2d 608. Although collection of personal information does not constitute "economic" injury for purposes of the CFAA, courts have recognized similar privacy violations as injuries for purposes of Section 349. See Meyerson v. Prime Realty Services, LLC, 7 Misc.3d 911, 920, 796 N.Y.S.2d 848 (N.Y.Sup.Ct.2005) ("[I]t cannot be doubted that a privacy invasion claim—and an accompanying request for attorney's fees-may be stated under [Section] 349 based on nonpecuniary injury ..."); Anonymous v. CVS Corp., 728 N.Y.2d 333, 340 (N.Y.Sup.Ct.2001) (allowing Section 349 claim for violation of privacy when local pharmacy transferred prescription records to a national chain without advance notice to consumers).

Plaintiff has therefore adequately pled a claim under Section 349 with respect to Defendant Interclick. Nevertheless, Plaintiff has not alleged any facts demonstrating that the Advertiser Defendants were involved in any of the allegedly deceptive conduct. Therefore, Defendant Interclick's Motion to Dismiss as to Plaintiff's Section 349 claim is DENIED, and the Advertiser Defendants' Motion to Dismiss the Section 349 claim is GRANTED.

…

III. CONCLUSION

For the above reasons, the Advertiser Defendants' Motion to Dismiss is GRANTED and Plaintiff's claims against McDonald's Corporation, CBS Corporation, Mazda Motor of America, Inc., Microsoft Corporation, and McDonald's USA, LLC, are dismissed with prejudice; Interclick's Motion to Dismiss is GRANTED with respect to Plaintiff's CFAA claim. Plaintiff's Breach of Implied Contract Claim, and Plaintiff's Tortious Interference with Contract claim, and those claims are dismissed with prejudice;

Interclick's Motion to Dismiss is DENIED with respect to Plaintiff's claim under New York General Business Law Section 349, and Plaintiff's Trespass to Chattels claim; and Defendant Interclick shall answer the remaining claims within 30 days of the date of this Order.

SO ORDERED.

Dwyer v. American Express Company

Appellate Court of Illinois,
First District, First Division.
June 30, 1995
273 Ill.App.3d 742
210 Ill.Dec. 375
652 N.E.2d 1351

Opinion

Justice BUCKLEY delivered the opinion of the court:

Plaintiffs, American Express cardholders, appeal the circuit court's dismissal of their claims for invasion of privacy and consumer fraud against defendants, American Express Company, American Express Credit Corporation, and American Express Travel Related Services Company, for their practice of renting **1353 ***377 information regarding cardholder spending habits.

On May 13, 1992, the New York Attorney General released a press statement describing an agreement it had entered into with defendants. The following day, newspapers reported defendants' actions which gave rise to this agreement. According to the news articles, defendants categorize and rank their cardholders into six tiers based on spending habits and then rent this information to participating merchants as part of a targeted joint-marketing and *744 sales program. For example, a cardholder may be characterized as “Rodeo Drive Chic” or “Value Oriented.” In order to characterize its cardholders, defendants analyze where they shop and how much they spend, and also consider behavioral characteristics and spending histories. Defendants then offer to create a list of cardholders who would most likely shop in a particular store and rent that list to the merchant.

Defendants also offer to create lists which target cardholders who purchase specific types of items, such as fine jewelry. The merchants using the defendants' service can also target shoppers in categories such as mail-order apparel buyers, home-improvement shoppers, electronics shoppers, luxury lodgers, card members with children, skiers, frequent business travelers, resort users, Asian/European travelers, luxury European car owners, or recent movers. Finally, defendants offer joint-marketing ventures to merchants who generate substantial sales through the American Express card. Defendants mail special promotions devised by the merchants to its cardholders and share the profits generated by these advertisements.

On May 14, 1992, Patrick E. Dwyer filed a class action against defendants. His complaint alleges that defendants intruded into their cardholders' seclusion, commercially appropriated their cardholders' personal spending habits, and violated the Illinois consumer fraud statute and consumer fraud statutes in other jurisdictions. Maria Teresa Rojas later filed a class action containing the same claims. The circuit court consolidated the two actions. Plaintiffs moved to certify the class, add parties, and file an amended, consolidated complaint. Defendants moved to dismiss the claims. The parties fully briefed the motions to dismiss and to certify the class. After

hearing argument on the motion to dismiss, the circuit court granted that motion and denied plaintiffs' motions as moot. Plaintiffs appeal the circuit court order.

Plaintiffs have alleged that defendants' practices constitute an invasion of their privacy and violate the Illinois Consumer Fraud and Deceptive Business Practices Act (Act or Consumer Fraud Act) (Ill.Rev.Stat.1991, ch. 121 ½, par. 261 et seq. (now 815 ILCS 505/1 et seq. (West 1992))). For the reasons discussed below, we find that plaintiffs have not stated a cause of action under either of these theories.

Invasion of Privacy

There are four branches of the privacy invasion tort identified by the Restatement (Second) of Torts. These are: (1) an unreasonable intrusion upon the seclusion of another; (2) an appropriation of *745 another's name or likeness; (3) a public disclosure of private facts; and (4) publicity which reasonably places another in a false light before the public. (Restatement (Second) of Torts §§ 652B, 652C, 652D, 652E, at 378-94 (1977); W. Keeton, Prosser & Keeton on Torts § 117, at 849-69 (5th ed. 1984).) Plaintiffs' complaint includes claims under the first and second branches.

As a preliminary matter, we note that a cause of action for intrusion into seclusion has never been recognized explicitly by the Illinois Supreme Court.
…
In 1979, this district declined to entertain a cause of action for intrusion into the seclusion of another in Kelly v. Franco (1979), 72 Ill.App.3d 642, 28 Ill.Dec. 855, 391 N.E.2d 54. In Kelly, the plaintiffs contended that the defendant repeatedly made phone calls to their home, only to hang up when one of the plaintiffs answered. The plaintiffs also alleged that the defendant verbally threatened and abused them and harassed their son. (Kelly, 72 Ill.App.3d at 644, 28 Ill.Dec. at 857, 391 N.E.2d at 56.) This court noted that the law in Illinois was inconsistent on this matter and held that even if it were to recognize such a cause of action the plaintiff's allegations were insufficient to support a cause of action for unreasonable intrusion into another's seclusion. Kelly, 72 Ill.App.3d at 646-47, 28 Ill.Dec. at 859, 391 N.E.2d at 58.

The third district recognized the intrusion tort in Melvin v. Burling (1986), 141 Ill.App.3d 786, 95 Ill.Dec. 919, 490 N.E.2d 1011, seven years after Kelly. In Melvin, the court set out four elements which must be alleged in order to state a cause of action: (1) an unauthorized intrusion or prying into the plaintiff's seclusion; (2) an intrusion which is offensive or objectionable to a reasonable man; (3) the matter upon *746 which the intrusion occurs is private; and (4) the intrusion causes anguish and suffering. (Melvin, 141 Ill.App.3d at 789, 95 Ill.Dec. at 921-22, 490 N.E.2d at 1013-14.) Since the third district set out the four elements in Melvin, this district has applied these elements without directly addressing the issue of whether the cause of action exists in this State. In Mucklow v. John Marshall Law School (1988), 176 Ill.App.3d 886, 126 Ill.Dec. 314, 531 N.E.2d 941, and again in Miller v. Motorola, Inc. (1990), 202 Ill.App.3d 976, 148 Ill.Dec. 303, 560 N.E.2d 900, this district held that the plaintiff's allegations did not satisfy the first element of Melvin, without expressing a view as to the conflict regarding the recognition of the cause of action. Mucklow, 176 Ill.App.3d at 894, 126 Ill.Dec. at 319, 531 N.E.2d at 946; Miller, 202 Ill.App.3d at 981-82, 148 Ill.Dec. at 307, 560 N.E.2d at 904.

Plaintiffs' allegations fail to satisfy the first element, an unauthorized intrusion or prying into the plaintiffs' seclusion. The alleged wrongful actions involve the defendants' practice of renting lists that they have compiled from information contained in their own records. By using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.

Plaintiffs claim that because defendants rented lists based on this compiled information, this case involves the disclosure of private financial information and most closely resembles cases involving intrusion into private financial dealings, such as bank account transactions. Plaintiffs cite several cases in which courts have recognized the right to privacy surrounding financial transactions. See Zimmermann v. Wilson (3d Cir.1936), 81 F.2d 847 (holding examination of information in taxpayers' bank books would violate the taxpayers' privacy rights); Brex v. Smith (1929), 104 N.J.Eq. 386, 146 A. 34 (upholding claim for unauthorized intrusion into the plaintiff's bank account); Hickson v. Home Federal (N.D.Ga.1992), 805 F.Supp. 1567 (finding bank disclosure to credit bureau of borrower's loan payment delinquency could violate borrower's right to privacy); Suburban Trust Co. v. Waller (1979), 44 Md.App. 335, 408 A.2d 758 (holding bank cannot reveal information about customers' account or transaction unless compelled by legal process); Mason v. Williams Discount Center, Inc. (Mo.1982), 639 S.W.2d 836 (finding **1355 ***379 store's posting of names of bad check risks invades plaintiff's privacy).

However, we find that this case more closely resembles the sale of magazine subscription lists, which was at issue in Shibley v. Time, Inc. (1975), 45 Ohio App.2d 69, 341 N.E.2d 337. In Shibley, the *747 plaintiffs claimed that the defendant's practice of selling and renting magazine subscription lists without the subscribers' prior consent “constitut[ed] an invasion of privacy because it amount[ed] to a sale of individual ‘personality profiles,’ which subjects the subscribers to solicitations from direct mail advertisers.” (Shibley, 45 Ohio App.2d at 71, 341 N.E.2d at 339.) The plaintiffs also claimed that the lists amounted to a tortious appropriation of their names and “personality profiles.” The trial court dismissed the plaintiffs' complaint and the Court of Appeals of Ohio affirmed. Shibley, 45 Ohio App.2d at 71, 341 N.E.2d at 339.

The Shibley court found that an Ohio statute, which permitted the sale of names and addresses of registrants of motor vehicles, indicated that the defendant's activity was not an invasion of privacy. The court considered a Federal district court case from New York, Lamont v. Commissioner of Motor Vehicles (S.D.N.Y.1967), 269 F.Supp. 880, aff'd (2d Cir.1967) 386 F.2d 449 cert. denied (1968), 391 U.S. 915, 88 S.Ct. 1811, 20 L.Ed.2d 654, to be insightful. In Lamont, the plaintiff claimed an invasion of privacy arising from the State's sale of its list of names and addresses of registered motor-vehicle owners to mail-order advertisers. The Lamont court held that however “noxious” advertising by mail might be, the burden was acceptable as far as the Constitution is concerned. (Lamont, 269 F.Supp. at 883.) The Shibley court followed the reasoning in Lamont and held:

> "The right to privacy does not extend to the mailbox and therefore it is constitutionally permissible to sell subscription lists to direct mail advertisers. It necessarily follows that the practice complained of here does not constitute an invasion of privacy even if appellants' unsupported assertion that this amounts to the sale of 'personality profiles' is taken as true because these profiles are only used to determine what type of advertisement is to be sent." Shibley, 45 Ohio App.2d at 73, 341 N.E.2d at 339-40.

Defendants rent names and addresses after they create a list of cardholders who have certain shopping tendencies; they are not disclosing financial information about particular cardholders. These lists are being used solely for the purpose of determining what type of advertising should be sent to whom. We also note that the Illinois Vehicle Code authorizes the Secretary of State to sell lists of names and addresses of licensed drivers and registered motor-vehicle owners. (625 ILCS 5/2-123 (West 1992).) Thus, we hold that the alleged actions here do not constitute an unreasonable intrusion into the seclusion of another. We so hold without expressing a view as to the appellate court conflict regarding the recognition of this cause of action.

*748 234 Considering plaintiffs' appropriation claim, the elements of the tort are: an appropriation, without consent, of one's name or likeness for another's use or benefit. (Restatement (Second) of Torts § 652C (1977); Leopold v. Levin (1970), 45 Ill.2d 434, 444, 259 N.E.2d 250, 256.) This branch of the privacy doctrine is designed to protect a person from having his name or image used for commercial purposes without consent. (See Douglass v. Hustler Magazine (7th Cir.1985), 769 F.2d 1128, cert. denied (1986), 475 U.S. 1094, 106 S.Ct. 1489, 89 L.Ed.2d 892 (finding defendant appropriated the value of model's likeness when it published nude pictures of her without consent).) According to the Restatement, the purpose of this tort is to protect the "interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness." (Restatement (Second) of Torts § 652C, Comment a (1977).) Illustrations of this tort provided by the Restatement include the publication of a person's photograph without consent in an advertisement; operating a corporation named after a prominent public figure without the person's consent; impersonating a man to obtain information regarding the affairs of the man's wife; and filing a lawsuit in the name of another without the **1356 ***380 other's consent. Restatement (Second) of Torts § 652C, Comment b (1965).

Plaintiffs claim that defendants appropriate information about cardholders' personalities, including their names and perceived lifestyles, without their consent. Defendants argue that their practice does not adversely affect the interest of a cardholder in the "exclusive use of his own identity," using the language of the Restatement. Defendants also argue that the cardholders' names lack value and that the lists that defendants create are valuable because "they identify a useful aggregate of potential customers to whom offers may be sent."

Defendants cite Cox v. Hatch (Utah 1988), 761 P.2d 556, to support their argument. In Cox, the supreme court of Utah held that there had been no wrongful appropriation of plaintiffs' images through use of their pictures in campaign advertisements because the plaintiffs did not allege that their images had any intrinsic value or that they enjoyed any particular fame or notoriety. (Cox, 761 P.2d at 564.) Even more persuasive is Shibley v. Time, Inc. (1975), 45 Ohio App.2d 69, 341 N.E.2d 337, discussed above, wherein the Court of Appeals of Ohio found that merely placing a

person's name on a “personality profile” list and providing that list to a third party, did not constitute tortious appropriation. Shibley, 45 Ohio App.2d at 71, 341 N.E.2d at 339.

*749 To counter defendants' argument, plaintiffs point out that the tort of appropriation is not limited to strictly commercial situations. See Annerino v. Dell Publishing Co. (1958), 17 Ill.App.2d 205, 208, 149 N.E.2d 761 (implying that the holding of Eick v. Perk Dog Food Co. (1952), 347 Ill.App. 293, 106 N.E.2d 742, was being expanded beyond strictly commercial situations), and Douglass v. Hustler Magazine (7th Cir.1985), 769 F.2d 1128, 1138 (recognizing a good appropriation claim under Illinois law for commercial nonadvertising use of photographs); see also Zacchini v. Scripps-Howard Broadcasting Co. (1976), 47 Ohio St.2d 224, 351 N.E.2d 454, rev'd on other grounds (1977), 433 U.S. 562, 97 S.Ct. 2849, 53 L.Ed.2d 965, (holding that Ohio law does not limit appropriation claims to commercial appropriation).

Nonetheless, we again follow the reasoning in Shibley and find that plaintiffs have not stated a claim for tortious appropriation because they have failed to allege the first element. Undeniably, each cardholder's name is valuable to defendants. The more names included on a list, the more that list will be worth. However, a single, random cardholder's name has little or no intrinsic value to defendants (or a merchant). Rather, an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendants' practices do not deprive any of the cardholders of any value their individual names may possess.

Consumer Fraud Act

Plaintiffs' complaint also includes a claim under the Illinois Consumer Fraud Act. (Ill.Rev.Stat.1991, ch. 121 ½, par. 261 et seq. (now 815 ILCS 505/1 et seq. (West 1992)).) To establish a deceptive practice claim, a plaintiff must allege and prove (1) the misrepresentation or concealment of a material fact, (2) an intent by defendant that plaintiff rely on the misrepresentation or concealment, and (3) the deception occurred in the course of conduct involving a trade or commerce. Ill.Rev.Stat.1991, ch. 121 ½, par. 262 (now 815 ILCS 505/2 (West 1992)); Siegel v. Levy Organization Development Co. (1992), 153 Ill.2d 534, 542, 180 Ill.Dec. 300, 304, 607 N.E.2d 194, 198.

In Elder v. Coronet Insurance Co. (1990), 201 Ill.App.3d 733, 146 Ill.Dec. 978, 558 N.E.2d 1312, the defendant insurance company failed to inform its customers, at the time of sale of insurance policies, of its practice of denying automobile-theft claims on the basis of polygraph examinations. The court held that the plaintiff's assertion that the defendant failed to disclose its claims adjustment practices sufficiently alleged a deceptive practice under the Act. (Elder, 201 Ill.App.3d at 751, 146 Ill.Dec. at 987-89, 558 N.E.2d at 1321-23.) The court found this misrepresentation to be material because a customer would be expected to rely on this information *750 when making a decision to buy insurance from the defendant. **1357 ***381 Elder, 201 Ill.App.3d at 751, 146 Ill.Dec. at 988, 558 N.E.2d at 1322.

According to the plaintiffs, defendants conducted a survey which showed that 80% of Americans do not think companies should release personal information to other companies. Plaintiffs have alleged that defendants did disclose that it would use information provided in the credit card

application, but this disclosure did not inform the cardholders that information about their card usage would be used. It is highly possible that some customers would have refrained from using the American Express Card if they had known that defendants were analyzing their spending habits. Therefore, plaintiffs have sufficiently alleged that the undisclosed practices of defendants are material and deceptive.

789 As to the second element, the Act only requires defendants' intent that plaintiffs rely on the deceptive practice. Actual reliance is not required. (Siegel, 153 Ill.2d at 542, 180 Ill.Dec. at 304, 607 N.E.2d at 198.) “A party is considered to intend the necessary consequences of his own acts or conduct.” (Warren v. LeMay (1986), 142 Ill.App.3d 550, 566, 96 Ill.Dec. 418, 428, 491 N.E.2d 464, 474.) When considering whether this element is met, good or bad faith is not important and innocent misrepresentations may be actionable. (Warren, 142 Ill.App.3d at 566, 96 Ill.Dec. at 428, 491 N.E.2d at 474.) Defendants had a strong incentive to keep their practice a secret because disclosure would have resulted in fewer cardholders using their card. Thus, plaintiffs have sufficiently alleged that defendants intended for plaintiff's to rely on the nondisclosure of their practice.

The third element is not at issue in this case. However, defendants argue that plaintiffs have failed to allege facts that might establish that they suffered any damages. The Illinois Consumer Fraud Act provides a private cause of action for damages to “[a]ny person who suffers damage as a result of a violation of th[e] Act.” (Ill.Rev.Stat.1991, ch. 121 ½, par. 270a (now 815 ILCS 505/10a(a) (West 1992)).) Defendants contend, and we agree, that the only damage plaintiffs could have suffered was a surfeit of unwanted mail. We reject plaintiffs' assertion that the damages in this case arise from the disclosure of personal financial matters. Defendants only disclose which of their cardholders might be interested in purchasing items from a particular merchant based on card usage. Defendants' practice does not amount to a disclosure of personal financial matters. Plaintiffs have failed to allege how they were damaged by defendants' practice of selecting cardholders for mailings likely to be of interest to them.

*751 Plaintiffs argue that the consumer fraud statutes of other States allow recovery of mental anguish even if no other damages are pled or proved. Apparently, plaintiffs would like this court to assume that a third party's knowledge of a cardholder's interest in their goods or services causes mental anguish to cardholders. Such an assumption without any supporting allegations would be wholly unfounded in this case. Therefore, we hold that plaintiffs have failed to allege facts that might establish that they have suffered any damages as a result of defendants' practices. Accordingly, for the reasons set forth above, we affirm the order of the circuit court of Cook County.

Affirmed.
RAKOWSKI and CAHILL, JJ., concur.

Intel Corp. v. Hamidi

Supreme Court of California
June 30, 2003
30 Cal.4th 1342
1 Cal.Rptr.3d 32
71 P.3d 296

Opinion

WERDEGAR, J.

Intel Corporation (Intel) maintains an electronic mail system, connected to the Internet, through which messages between employees and those outside the company can be sent and received, and permits its employees to make reasonable nonbusiness use of this system. On six occasions over almost two years, Kourosh Kenneth Hamidi, a former Intel employee, sent e-mails criticizing Intel's employment practices to numerous current employees on Intel's electronic mail system. Hamidi breached no computer security barriers in order to communicate with Intel employees. He offered to, and did, remove from his mailing list any recipient who so wished. Hamidi's communications to individual Intel employees caused neither physical damage nor functional disruption to the company's computers, nor did they at any time deprive Intel of the use of its computers. The contents of the messages, however, caused discussion among employees and managers.

On these facts, Intel brought suit, claiming that by communicating with its employees over the company's e-mail system Hamidi committed the tort of ***1347*** trespass to chattels. ****300*** The trial court granted Intel's motion for summary judgment and enjoined Hamidi from any further mailings. A divided Court of Appeal affirmed.

After reviewing the decisions analyzing unauthorized electronic contact with computer systems as potential trespasses to chattels, we conclude that under California law the tort does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning. Such an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not interfere with the possessor's use or possession of, or any other legally protected interest in, the personal property itself. (See *Zaslow v. Kroenert* (1946) 29 Cal.2d 541, 551, 176 P.2d 1; *Ticketmaster Corp. v. Tickets.com, Inc.* (C.D.Cal., Aug. 10, 2000, No. 99CV7654) 2000 WL 1887522, p. *4; Rest.2d Torts, § 218.) The consequential economic damage Intel claims to have suffered, i.e., loss of productivity caused by employees reading and reacting to Hamidi's messages and company efforts to block the messages, is not an injury to the company's interest in its computers—which worked as intended and were unharmed by the communications—any more than the personal distress caused by reading an unpleasant letter would be an injury to the recipient's mailbox, or the loss of privacy caused by an intrusive telephone call would be an injury to the recipient's telephone equipment.

Our conclusion does not rest on any special immunity for communications by electronic mail; we do not hold that ***37** messages transmitted through the Internet are exempt from the ordinary rules of tort liability. To the contrary, e-mail, like other forms of communication, may in some circumstances cause legally cognizable injury to the recipient or to third parties and may be actionable under various common law or statutory theories. Indeed, on facts somewhat similar to those here, a company or its employees might be able to plead causes of action for interference with prospective economic relations (see *Guillory v. Godfrey* (1955) 134 Cal.App.2d 628, 630–632, 286 P.2d 474 [defendant berated customers and prospective customers of plaintiffs' cafe with disparaging and racist comments]), interference with contract (see *Blender v. Superior Court* (1942) 55 Cal.App.2d 24, 25–27, 130 P.2d 179 [defendant made false statements about plaintiff to his employer, resulting in plaintiff's discharge]) or intentional infliction of emotional distress (see *Kiseskey v. Carpenters' Trust for So. California* (1983) 144 Cal.App.3d 222, 229–230, 192 Cal.Rptr. 492 [agents of defendant union threatened life, health, and family of employer if he did not sign agreement with union].) And, of course, as with any other means of publication, third party subjects of e-mail communications may under appropriate facts make claims for ***1348** defamation, publication of private facts, or other speech-based torts. (See, e.g.,*Southridge Capital Management v. Lowry* (S.D.N.Y.2002) 188 F.Supp.2d 388, 394–396 [allegedly false statements in e-mail sent to several of plaintiff's clients support actions for defamation and interference with contract].) Intel's claim fails not because e-mail transmitted through the Internet enjoys unique immunity, but because the trespass to chattels tort—unlike the causes of action just mentioned—may not, in California, be proved without evidence of an injury to the plaintiff's personal property or legal interest therein.

Nor does our holding affect the legal remedies of Internet service providers (ISP's) against senders of unsolicited commercial bulk e-mail (UCE), also known as “spam.” (See *Ferguson v. Friendfinders, Inc.* (2002) 94 Cal.App.4th 1255, 1267, 115 Cal.Rptr.2d 258.) A series of federal district court decisions, beginning with *CompuServe, Inc. v. Cyber Promotions, Inc.* (S.D.Ohio 1997) 962 F.Supp. 1015, has approved the use of trespass to chattels as a theory of spammers' liability to ISP's, based upon evidence that the vast quantities of mail sent by spammers both overburdened the ISP's own computers and made the entire computer system harder to use for recipients, the ISP's customers. (See *id.* at pp. 1022–1023.) In those cases, discussed in greater detail below, the underlying complaint was that the extraordinary *quantity* of UCE impaired the computer system's functioning. In the present case, the claimed injury is located in the disruption***301** or distraction caused to recipients by the *contents* of the e-mail messages, an injury entirely separate from, and not directly affecting, the possession or value of personal property.

…

DISCUSSION

I. Current California Tort Law

Dubbed by Prosser the “little brother of conversion,” the tort of trespass to chattels allows recovery for interferences with possession of personal property “not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered.” (Prosser & Keeton, Torts (5th ed.1984) § 14, pp. 85–86.)

Though not amounting to conversion, the defendant's interference must, to be actionable, have caused some injury to the chattel or to the plaintiff's rights in it. Under California law, trespass to chattels "lies where an intentional interference with the possession of personal property *has proximately* ***1351** *caused injury.*" (*Thrifty–Tel, Inc. v. Bezenek* (1996) 46 Cal.App.4th 1559, 1566, 54 Cal.Rptr.2d 468, italics added.) In cases of interference with possession of personal property not amounting to conversion, "the owner has a cause of action for trespass or case, *and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use.*" (*Zaslow v. Kroenert, supra,* 29 Cal.2d at p. 551, 176 P.2d 1, italics added; accord, *Jordan v. Talbot* (1961) 55 Cal.2d 597, 610, 12 Cal.Rptr. 488, 361 P.2d 20.) In modern American law generally, "[t]respass remains as an occasional remedy for minor interferences, *resulting in some damage,* but not sufficiently serious or sufficiently important to amount to the greater tort" of conversion. (Prosser & Keeton, Torts, *supra,* § 15, p. 90, italics added.)

…

Intel suggests that the requirement of actual harm does not apply here because it sought only injunctive relief, as protection from future injuries. But as Justice Kolkey, dissenting below, observed, "[t]he fact the relief sought is injunctive does not excuse a showing of injury, whether actual or threatened." Indeed, in order to obtain injunctive relief the plaintiff must ordinarily show that the defendant's wrongful acts threaten to cause *irreparable* injuries, ones that cannot be adequately compensated in damages. (5 Witkin, Cal. Procedure (4th ed. 1997) Pleading, § 782, p. 239.) Even in an action for trespass to real property, in which damage to the property is not an ***41** element of the cause of action, "the extraordinary remedy of injunction" cannot be invoked without showing the likelihood of irreparable harm. (*Mechanics' Foundry v. Ryall* (1888) 75 Cal. 601, 603, 17 P. 703; see *Mendelson v. McCabe* (1904) 144 Cal. 230, 232–233, 77 P. 915 [injunction against trespass to land proper where continued trespasses threaten creation of prescriptive right and repetitive suits for damages would be inadequate remedy].) A fortiori, to issue an injunction without a showing of likely irreparable injury in an action for trespass to chattels, in which injury to the personal property or the possessor's interest in it *is* an element of the action, would make little legal sense.

The dispositive issue in this case, therefore, is whether the undisputed facts demonstrate Hamidi's actions caused or threatened to cause damage to Intel's computer system, or injury to its rights in that personal property, such as to entitle Intel to judgment as a matter of law. To review, the undisputed ***1353** evidence revealed no actual or threatened damage to Intel's computer hardware or software and no interference with its ordinary and intended operation. Intel was not dispossessed of its computers, nor did Hamidi's messages prevent Intel from using its computers for any measurable length of time. Intel presented no evidence its system ****304** was slowed or otherwise impaired by the burden of delivering Hamidi's electronic messages. Nor was there any evidence transmission of the messages imposed any marginal cost on the operation of Intel's computers. In sum, no evidence suggested that in sending messages through Intel's Internet connections and internal computer system Hamidi used the system in any manner in which it was not intended to function or impaired the system in any way. Nor does the evidence show the request of any employee to be removed from FACE–Intel's mailing list was not honored. The evidence did show, however, that some employees who found the messages unwelcome asked management to stop them and that Intel technical staff spent time and effort attempting to block

the messages. A statement on the FACE–Intel Web site, moreover, could be taken as an admission that the messages had caused "[e]xcited and nervous managers" to discuss the matter with Intel's human resources department.
…
***45** In addition to impairment of system functionality, *CompuServe* and its progeny also refer to the ISP's loss of business reputation and customer goodwill, resulting from the inconvenience and cost that spam causes to its members, as harm to the ISP's legally protected interests in its personal property. (See *CompuServe, supra,* 962 F.Supp. at p. 1023; *Hotmail Corp. v. Van$ Money Pie, Inc., supra,* 1998 WL 388389 at p. *7; *America Online, Inc. v. IMS, supra,* 24 F.Supp.2d at p. 550.) Intel argues that its own interest in employee productivity, assertedly disrupted by Hamidi's messages, is a comparable protected interest in its computer system. We disagree.
…
This theory of "impairment by content" (Burk, *The Trouble with Trespass, supra,* 4 J. Small & Emerging Bus.L. at p. 37) threatens to stretch trespass ***1359** law to cover injuries far afield from the harms to possession the tort evolved to protect. Intel's theory would expand the tort of trespass to chattels to cover virtually any unconsented—to communication that, solely because of its content, is unwelcome to the recipient or intermediate transmitter. As the dissenting justice below explained, " 'Damage' of this nature—the distraction of reading or listening to an unsolicited communication—is not within the scope of the injury against which the trespass-to-chattel tort protects, and indeed trivializes it. After all, '[t]he property interest protected by the old action of trespass was that of possession; and this has continued to affect the character of the action.' (Prosser & Keeton on Torts, *supra,* § 14, p. 87.) Reading an e-mail transmitted to equipment designed to receive it, in and of itself, does not affect the possessory interest in the equipment. [¶] Indeed, if a chattel's receipt of an electronic communication constitutes a trespass to that chattel, then not only are unsolicited telephone calls and faxes trespasses to chattel, but unwelcome radio waves and television signals also constitute a trespass to chattel every time the viewer inadvertently sees or hears the unwanted program." We agree. While unwelcome communications, electronic or otherwise, can cause a variety of injuries to economic relations, reputation and emotions, those interests are protected by other branches of tort law; in order to address them, we need not create a fiction of injury to the communication system.

Nor may Intel appropriately assert a *property* interest in its employees' time. "The Restatement test clearly speaks in the first instance to the impairment of the chattel.... But employees are not chattels (at least not in the legal sense of the term)." (Burk, *The Trouble with Trespass, supra,* 4 J. Small & Emerging Bus.L. at p. 36.) Whatever interest Intel may have in preventing its employees from receiving disruptive communications, it is not an interest in personal property, and trespass to chattels is therefore not an action that will lie to protect it. Nor, finally, can the fact Intel staff spent time attempting to block Hamidi's messages be bootstrapped into an injury to Intel's possessory interest in its computers. To quote, again, from the dissenting opinion in the Court of Appeal: "[I]t is circular to premise the damage element of a tort solely upon the steps taken to prevent the damage. Injury can only be established by the completed tort's consequences, not by the cost of the steps taken to avoid the injury and prevent the tort; otherwise, we can create injury for every supposed tort."

Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company ***47** necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other companies and individuals. That some communications *1360* would, because of their contents, be unwelcome to Intel management was virtually inevitable. Hamidi did nothing but use the e-mail system for its intended purpose—to communicate with employees. The system worked as designed, delivering the messages without any physical or functional harm or disruption. These occasional transmissions cannot reasonably be viewed as impairing the quality or value of Intel's computer system. We conclude, therefore, that Intel has not presented undisputed facts demonstrating an injury to its personal property, or to its legal interest in that property, that support, under California tort law, an action for trespass to chattels.

II. Proposed Extension of California Tort Law

We next consider whether California common law should be *extended* to cover, as a trespass to chattels, an otherwise harmless electronic communication whose contents are objectionable. We decline to so expand California law. Intel, of course, was not the recipient of Hamidi's messages, but rather **309* the owner and possessor of computer servers used to relay the messages, and it bases this tort action on that ownership and possession. The property rule proposed is a rigid one, under which the sender of an electronic message would be strictly liable to the owner of equipment through which the communication passes—here, Intel—for any consequential injury flowing from the *contents* of the communication. The arguments of amici curiae and academic writers on this topic, discussed below, leave us highly doubtful whether creation of such a rigid property rule would be wise.

Writing on behalf of several industry groups appearing as amici curiae, Professor Richard A. Epstein of the University of Chicago urges us to excuse the required showing of injury to personal property in cases of unauthorized electronic contact between computers, "extending the rules of trespass to real property to all interactive Web sites and servers." The court is thus urged to recognize, for owners of a particular species of personal property, computer servers, the same interest in inviolability as is generally accorded a possessor of land. In effect, Professor Epstein suggests that a company's server should be its castle, upon which any unauthorized intrusion, however harmless, is a trespass.

Epstein's argument derives, in part, from the familiar metaphor of the Internet as a physical space, reflected in much of the language that has been used to describe it: "cyberspace," "the information superhighway," e-mail "addresses," and the like. Of course, the Internet is also frequently called simply the "Net," a term, Hamidi points out, "evoking a fisherman's chattel." A major component of the Internet is the World Wide "Web," a *1361* descriptive term suggesting neither personal nor real property, and "cyberspace" itself has come to be known by the oxymoronic phrase "virtual reality," which would suggest that any real property "located" in "cyberspace" must be "virtually real" property. Metaphor is a two-edged sword.
…
The plain fact is that computers, even those making up the Internet, are—like such older communications equipment as telephones and fax machines—personal property, not realty.

Professor Epstein observes that "[a]lthough servers may be moved in real space, they cannot be moved in cyberspace," because an Internet server must, to be useful, be accessible at a known address. But the same is true of the telephone: to be useful for incoming communication, the telephone must remain constantly linked to the same number (or, when the number is changed, the system must include some forwarding or notification capability, a qualification that also applies to computer addresses). Does this suggest that an unwelcome message delivered through a telephone or fax machine should be viewed as a trespass to a type of real property? We think not: As already discussed, the contents of a telephone communication may cause a variety of injuries and may be the basis for a variety of tort actions (e.g., defamation, intentional infliction of emotional distress, invasion of privacy), *****310*** but the injuries are not to an ****1362*** interest in property, much less real property, and the appropriate tort is not trespass.[7]

…
****1364*** The Legislature has already adopted detailed regulations governing UCE. (Bus. & Prof.Code, §§ 17538.4, 17538.45; see generally *Ferguson v. Friendfinders, Inc., supra,* 94 Cal.App.4th 1255, 115 Cal.Rptr.2d 258.) It may see fit in the future also to regulate noncommercial e-mail, such as that sent by Hamidi, or other kinds of unwanted contact between computers on the Internet, such as that alleged in *eBay, supra,* 100 F.Supp.2d 1058. But we are not persuaded that these perceived problems call at present for judicial creation of a rigid property rule of computer server inviolability. We therefore decline to create an exception, covering Hamidi's unwanted electronic messages to Intel employees, to the general rule that a trespass to chattels is not actionable if it does not involve actual or threatened injury to the personal property or to the possessor's legally protected interest in the personal property. No such injury having been shown on the undisputed facts, Intel was not entitled to summary judgment in its favor.

…
Dissenting Opinion of BROWN, J.

Candidate A finds the vehicles that candidate B has provided for his campaign workers, and A spray paints the water soluble message, "Fight corruption, vote for A" on the bumpers. The majority's reasoning would find that notwithstanding the time it takes the workers to remove the paint and the expense they incur in altering the bumpers to prevent further unwanted messages, candidate B does not deserve an injunction unless the paint is so heavy that it reduces the cars' gas mileage or otherwise depreciates the cars' market value. Furthermore, candidate B has an obligation to permit the paint's display, because the cars are driven by workers and not B personally, because B allows his workers to use the cars to pick up their lunch or retrieve their children from school, or because the bumpers display B's own slogans. I disagree.

Intel has invested millions of dollars to develop and maintain a computer system. It did this not to act as a public forum but to enhance the productivity of its employees. Kourosh Kenneth Hamidi sent as many as 200,000 e-mail messages to Intel employees. The time required to review and delete Hamidi's messages diverted employees from productive tasks and undermined the utility of the computer system. "There may ... be situations in which the value to the owner of a particular*****53*** type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition." (Rest.2d Torts, § 218, com. h, p. 422.) This is such a case.

The majority repeatedly asserts that Intel objected to the hundreds of thousands of messages solely due to their content, and proposes that Intel seek relief by pleading content-based speech torts. This proposal misses the point that Intel's objection is directed not toward Hamidi's message but his use of Intel's property to display his message. Intel has not sought to prevent Hamidi from expressing his ideas on his Web site, through private mail (paper or electronic) to employees' homes, or through any other means like picketing or billboards. But as counsel for Intel explained during oral ***1368*** argument, the company objects to Hamidi's using Intel's property to advance his message.

Of course, Intel deserves an injunction even if its objections are based entirely on the e-mail's content. Intel is entitled, for example, to allow employees use of the Internet to check stock market tables or weather forecasts without incurring any concomitant obligation to allow access to pornographic Web sites. ***314** (*Loving v. Boren* (W.D.Okla.1997) 956 F.Supp. 953, 955.) A private property owner may choose to exclude unwanted mail for any reason, including its content. (*Rowan v. U.S. Post Office Dept.* (1970) 397 U.S. 728, 738, 90 S.Ct. 1484, 25 L.Ed.2d 736 (*Rowan*); *Tillman v. Distribution Systems of America Inc.* (1996) 224 A.D.2d 79, 648 N.Y.S.2d 630, 635 (*Tillman*).)

The majority refuses to protect Intel's interest in maintaining the integrity of its own system, contending that (1) Hamidi's mailings did not physically injure the system; (2) Intel receives many unwanted messages, of which Hamidi's are but a small fraction; (3) Intel must have contemplated that it would receive some unwanted messages; and (4) Hamidi used the e-mail system for its intended purpose, to communicate with employees.

Other courts have found a protectable interest under very similar circumstances. In *Thrifty–Tel v. Bezenek* (1996) 46 Cal.App.4th 1559, 54 Cal.Rptr.2d 468 (*Thrifty–Tel*), the Court of Appeal found a trespass to chattels where the defendants used another party's access code to search for an authorization code with which they could make free calls. The defendants' calls did not damage the company's system in any way; they were a minuscule fraction of the overall communication conducted by the phone network; and the company could have reasonably expected that some individuals would attempt to obtain codes with which to make free calls (just as stores expect shoplifters). Moreover, had the defendants succeeded in making free calls, they would have been using the telephone system as intended. (*Id.* at p. 1563, 54 Cal.Rptr.2d 468.) Because I do not share the majority's antipathy toward property rights and believe the proper balance between expressive activity and property protection can be achieved without distorting the law of trespass, I respectfully dissent.

…

THE TRIAL COURT CORRECTLY ISSUED THE INJUNCTION

Intel had the right to exclude the unwanted speaker from its property, which Hamidi does not dispute; he does not argue that he has a right to force unwanted messages on Intel. The instant case thus turns on the question of whether Intel deserves a remedy for the continuing violation of its rights. I believe it does, and as numerous cases have demonstrated, an injunction to prevent a trespass to chattels is an appropriate means of enforcement.

The majority does not find that Hamidi has an affirmative right to have Intel transmit his messages, but denies Intel any remedy. Admittedly, the case would be easier if precise statutory provisions supported relief, but in the rapidly changing world of technology, in which even technologically savvy providers like America Online and CompuServe are one step behind spammers, the Legislature will likely remain three or four steps behind. In ***1375*** any event, the absence of a statutory remedy does not privilege Hamidi's interference with Intel's property. Nor are content-based speech torts adequate for violations of property rights unrelated to the speech's content. In any event, the possibility of another avenue for relief does not preclude an injunction for trespass to chattels.

The majority denies relief on the theory that Intel has failed to establish the requisite actual injury. As discussed, *post*, however, the injunction was properly ***59*** granted because the rule requiring actual injury pertains to damages, not equitable relief, and thus courts considering comparable intrusions have provided injunctive relief without a showing of actual injury. Furthermore, there was actual injury as (1) Intel suffered economic loss; (2) it is sufficient for the injury to impair the chattel's utility to the owner rather than the chattel's market value; and (3) even in the absence of any injury to the owner's utility, it is nevertheless a trespass where one party expropriates for his own use the resources paid for by another.

…

CONCLUSION

Those who have contempt for grubby commerce and reverence for the rarified ***67*** heights of intellectual discourse may applaud today's decision, but even the flow of ideas will be curtailed if the right to exclude is denied. As the Napster controversy revealed, creative individuals will be less inclined to develop intellectual property if they cannot limit the terms of its transmission. Similarly, if online newspapers cannot charge for access, they will be unable to pay the journalists and editorialists who generate ideas for public consumption.

This connection between the property right to objects and the property right to ideas and speech is not novel. James Madison observed, “a man's land, or merchandize, or money is called his property.” (Madison, *Property*, Nat. Gazette (Mar. 27, 1792), reprinted in The Papers of James Madison (Robert A. Rutland et al. edits.1983) p. 266, quoted in McGinnis, *The Once and Future Property–Based Vision of the First Amendment* (1996) 63 U.Chi. L.Rev. 49, 65.) Likewise, “a man has a property in his opinions and the free communication of them.” (*Ibid.*) Accordingly, “freedom of speech and property rights were seen simply as different aspects of an indivisible concept of liberty.” (*Id.* at p. 63.)

The principles of both personal liberty and social utility should counsel us to usher the common law of property into the digital age.

In re Google Privacy Policy Litigation

United States District Court,
N.D. California, San Jose Division.
December 28, 2012
2012 WL 6738343
No. C 12–01382 PSG.

Opinion

ORDER GRANTING DEFENDANT'S MOTION TO DISMISS WITH LEAVE TO AMEND

PAUL S. GREWAL, United States Magistrate Judge.

*1 In this putative consumer privacy class action, Defendant Google, Inc. (“Google”) moves to dismiss Plaintiffs Robert B. Demars, Lorena Barios, Nicholas Anderson, Matthew Villani, Scott McCullough, David Nisenbaum, Pedro Marti, and Allison C. Weiss's (collectively, “Plaintiffs”) consolidated compl ai nt.1 In light of Plaintiffs' concessions in their opposition,2 the operative complaint alleges violations of the Wiretap Act, 18 U.S.C. 2511 et seq., California's Right of Publicity Statute, Cal. Civ.Code 3344, California's Unfair Competition Law, Cal. Bus. & Prof.Code 17200 et seq., California's Consumer Legal Remedies Act, Cal. Civ.Code 1750 et seq., common law breach of contract, common law intrusion upon seclusion, common law commercial misappropriation, and violation of consumer protection laws of the various states. The parties appeared for hearing. Having studied the papers and considered the arguments of counsel, the court GRANTS Google's motion to dismiss with leave to amend.

I. BACKGROUND

Unless otherwise noted, the following allegations are taken from the consolidated complaint and are presumed true for purposes of ruling on the pending motion.

Plaintiffs bring this nationwide class action against Google on behalf of all persons and entities in the United States who acquired a Google account between August 19, 2004 and February 29, 2012 and maintained such an account until on or after March 1, 2012.3 Before March 1, 2012, Google maintained approximately 70 separate privacy policies for each of its products, each of which confirmed that Google used a consumer's personal information for only that particular product. On March 1, 2012, Google announced that it was eliminating the majority of its separate privacy policies in favor of a single, universal privacy policy that allows Google to crossreference and use consumers' personal information across multiple Google products. Google explained the basis for the change in policy as follows:

> The main change is for consumers with Google Accounts ... Our new Privacy Policy makes clear that, if you're signed in, we may combine information that you've provided from one service with information from other services. In short, we'll treat you as a single user across all our products, which will mean simpler, more intuitive Google experience.

In other words, Google may now combine information collected from a consumer's Gmail account with information collected from that consumer's Google search queries, along with the consumer's activities on other Google products, such as YouTube, Picasa, Maps, Docs, and Reader. According to Plaintiffs, in violation of its prior policies, Google now combines across its products logs of the following consumer information, without consumer consent:

- first and last name;
- home or other physical address (including street name and city);
- current, physical location, a consumer's email address, and other online contact information (such as the identifier or screen name);

*2

- IP address;
- telephone number (both home and mobile numbers);
- list of contacts;
- search history from Google's search engine;
- web surfing history from cookies placed on the computer; and
- posts on Google+.

Plaintiffs contend that Google's new policy violates its prior policies because the new policy no longer allows consumers to keep information gathered from one Google product separate from information gathered from other Google products. Plaintiffs further contend that Google's new policy violates consumers' privacy rights by allowing Google to take information from a consumer's Gmail account and Google+ account, for which consumers may have one expectation of privacy, for use in a different context, such as to personalize Google search engine results, or to personalize advertisements shown while a consumer is surfing the internet, products for which a consumer may have an entirely different expectation of privacy.[5]

Plaintiffs allege that they each acquired a Gmail account before the March 1, 2012 announcement of the new policy. Plaintiffs also allege that that they each purchased an Android powered mobile phone before the March 1 date, that they did not consent to Google's post-March 1 data aggregation activities, and that they received no compensation for these activities.

II. LEGAL STANDARDS

To satisfy Article III, a plaintiff "must show that (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."[8] A suit brought by a plaintiff without Article III standing is not a "case or controversy," and an Article III federal court therefore lacks subject matter jurisdiction over the suit.[9] In that event, the suit should be dismissed under Rule 12(b)(1).[10] The injury required by Article III may exist by virtue of "statutes creating legal rights, the invasion of which creates standing."[11] In such cases, the "standing question ... is whether the constitutional or standing provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief."[12]

…

III. DISCUSSION

…

*5 Plaintiffs' current allegations fall short ... Plaintiffs have not identified a concrete harm from the alleged combination of their personal information across Google's products and contrary to Google's previous policy sufficient to create an injury in fact. As Judge Koh noted in In re iPhone Application Litig.,[47] a recent case from the Central District of California is instructive.[48] In Spectrum Media, the plaintiffs accused an online third-party advertising network of installing cookies on their computers to circumvent user privacy controls and to track internet use without user knowledge or consent. The court held that the plaintiffs lacked Article III standing because (1) they had not alleged that any named plaintiff was actually harmed by the defendant's alleged conduct and (2) they had not alleged any "particularized example" of economic injury or harm to their computers, but instead offered only abstract concepts, such as "opportunity costs," "value-for-value exchanges," "consumer choice," and "diminished performance."[49] Other cases have held the same.[50]

Plaintiffs' arguments to the contrary are not persuasive. These arguments all reduce to the central notion that, in contrast to the plaintiffs in each of the cases discuss above, Plaintiffs here have alleged cognizable, non-pecuniary harm in addition to pecuniary damages by virtue of Google's statutory and common law violations. But a careful review of these cases proves this assertion to be false. For example, like Plaintiffs here, the plaintiffs in In re iPhone Application Litig. also brought claims under statutes like California's Consumer Legal Remedies Act and California's Unfair Competition Law as well as common law claims.[51] Similarly, in Low, the plaintiff argued that the loss of personal information, even in the absence of any cognizable economic harm, was sufficient to confer Article III standing. But as Judge Koh explained, nothing in the precedent of the Ninth Circuit or other appellate courts confers standing on a party that has brought statutory or common law claims based on nothing more than the unauthorized disclosure of personal information, let alone an unauthorized disclosure by a defendant to itself.[52]

…

As Judge Koh and the Central Distict both have observed, "[i]t is not obvious that Plaintiffs cannot articulate some actual or imminent injury in fact. It is just that at this point they haven't offered a coherent and factually supported theory of what that injury might be."[58]

In light of Plaintiffs' failure to allege fact sufficient to confer Article III standing, the court must refrain from addressing the remainder of Google's arguments and instead respect its lack of jurisdiction.

IV. CONCLUSION

Google's motion to dismiss is GRANTED with leave to amend. Plaintiffs shall file any amended complaint no later than January 31, 2012.

IT IS SO ORDERED.

Footnotes

…

5. According to Plaintiffs, the Federal Trade Commission ("FTC") previously found Google deceptively claimed that it would seek the consent of consumers before using their information for a purpose other than for which it was collected, and that Google had misrepresented consumers' ability to exercise control over their information. On October 11, 2011, Google and the FTC entered into a consent order to resolve the matter.
…
8. See Friends of the Earth, Inc. v. Laidlaw Envtl. Sys. (TOC), Inc., 528 U.S. 167, 180–181, 120 S.Ct. 693, 145 L.Ed.2d 610 (2000).
9. Steel Co. v. Citizens for a Better Environment, 523 U.S. 83, 101, 118 S.Ct. 1003, 140 L.Ed.2d 210 (1998).
10. See id. at 109–110.
11. See Edwards v. First Am. Corp., 610 F.3d 514, 517 (9th Cir.2010) (quoting Warth v. Seldin, 422 U.S. 490, 500, 95 S.Ct. 2197, 45 L.Ed.2d 343 (1975)).
12. See id.
…
47. Case No. 11–MD–02250–LHK, 2011 WL 4403963 (N.D.Cal. Sept.20, 2011).
48. See Genevive La Court v. Specific Media, Case No. SACV–10–1256–JW, 2011 WL 1661532, (C.D.Cal. Apr.28, 2011).
49. Specific Media, 2011 WL 1661532, at *7–13.
50. See In re Doubleclick, Inc. Privacy Litig., 154 F.Supp.2d 497, 525 (S.D.N.Y.2001) (holding that unauthorized collection of personal information by a third party is not "economic loss"); In re JetBlue Airways Corp. Privacy Litig., 379 F.Supp.2d 299, 327 (E.D.N.Y.2005) (holding that airline's disclosure of passenger data to third party in violation of airline's privacy policy had no compensable value); In re iPhone Application Litig., 2011 WL 4403963, at *4–6 (holding that undifferentiated "lost opportunity costs" and "value-for-value exchanges" resulting from collection and tracking of personal information were not cognizable injuries in fact); Low v. LinkedIn Corp., Case No. 11–CV–01468–LHK, 2011 WL 5509848, at *4 (N.D.Cal. Nov.11, 2011) (rejecting sufficiency of independent economic value of personal information to establish injury in fact).
51. See In re iPhone Application Litig., 2011 WL 4403963, at *3.
52. See Low, 2011 WL 5509848, at *6 (discussing Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir.2010); Pisciotti v. Old Nat'l Bankcorp, 499 F.3d 629, 634 (7th Cir.2007)).
…
58. In re iPhone Application Litig., 2011 WL 4403963, at *6 (quoting Specific Media, 2011 WL 1661532, at *6).

In re iPhone Application Litigation

United States District Court,
N.D. California, San Jose Division.
June 12, 2012
844 F.Supp.2d 1040

Opinion

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTIONS TO DISMISS

LUCY H. KOH, District Judge.

…
Plaintiffs ***1049*** claim that Defendants violated their privacy rights by unlawfully allowing third party applications ("apps") that run on the iDevices to collect and make use of, for commercial purposes, personal information without user consent or knowledge. … Plaintiffs' claims against the Mobile Industry Defendants for violations of the Stored Communications Act, violations of the California Constitutional right to privacy, violations of the Computer Fraud and Abuse Act, trespass, conversion, and unjust enrichment are dismissed. Plaintiffs' claims against Apple for violations of the Stored Communications Act, violations of the Wiretap Act, violations of the California Constitutional right to privacy, negligence, violations of the Computer Fraud and Abuse Act, trespass, conversion, and unjust enrichment are dismissed. For the reasons set forth in Section III.D., these claims are dismissed with prejudice. Plaintiffs' claims against Apple for violations of the Consumer Legal Remedies Act and the Unfair Competition Law survive Apple's motion to dismiss.

I. BACKGROUND

A. Factual Background

Unless otherwise noted, the following allegations are taken from the Amended Consolidated Complaint and are presumed to be true for purposes of ruling upon Defendants' motions to dismiss. Generally speaking, Plaintiffs' Amended Consolidated Complaint asserts claims with respect to two separate putative classes of individuals and challenges two separate aspects of the iDevices used by Plaintiffs.

The iDevice Class[2]

iDevices enable users to download apps via Apple's "App Store" application and website. First Amended Consolidated Complaint ("AC") ¶ 86. Apple exercises significant control over the apps that are available in its store. *Id.* ¶¶ 123–126. Apple's App Store has set Apple products apart from Apple's competitors: "[i]n the post 3G 2.0 iOS era, the success of Apple's iPhones sales [sic] is inextricably linked to consumers' access to its App Store." *Id.* ¶ 86. Apple represents to users of the App Store that it "takes precautions—including administrative, technical, and

physical measures—to safeguard your personal information against theft, loss, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction." *Id.* ¶ 78.

Although the apps at issue in this litigation are provided for free, Plaintiffs contend that they in fact pay a price for the use of the "free" apps because these Apple-approved apps allow their personal data to be collected from their iDevices. AC ¶¶ 1; 160. Plaintiffs allege that Apple designs its mobile devices to allow personal information to be disclosed to the Mobile Industry Defendants. *Id.* ¶¶ 159–60. "When users download and install the Apps on their iDevices the [Mobile Industry Defendants'] software accesses personal ****1050*** information on those devices without users' awareness or permission and transmits the information to the [Mobile Industry Defendants]." *Id.* ¶ 161. The information collected by Defendants includes Plaintiffs' addresses and current whereabouts; the unique device identifier ("UDID") assigned to the iDevice; the user's gender, age, zip code and time zone; and app-specific information such as which functions Plaintiff performed on the app. *Id.* ¶ 2; *see also id.* ¶¶ 53–67, 161. These practices have allowed the Mobile Industry Defendants to "acquire details about consumers and to track consumers on an ongoing basis, across numerous applications and tracking consumers when they accessed Apps from different mobile devices." *Id.* ¶ 164.

Plaintiffs allege that, in light of Apple's public statements about protecting user privacy, Plaintiffs did not expect or consent to the Mobile Industry Defendants' tracking and collecting their app use or otherwise personal information. *Id.* ¶ 173–74. Moreover, Plaintiffs allege that they consider the information about their mobile communications to be personal and confidential. *Id.* ¶ 177.

Plaintiffs assert that these practices have led to several concrete harms to the "iDevice Class," defined as "[a]ll persons residing in the United States who have purchased iPhones and downloaded free Apps from the App Store on a mobile device that runs Apple's iOS, from December 1, 2008 to the date of the filing of this Complaint." AC ¶ 203. For one, the Mobile Industry Defendants' actions have consumed finite resources in the form of bandwidth and storage space on their iDevices. *Id.* ¶ 198. For example, downloading the Weather Channel App "caused a compressed.zip file of approximately two megabytes in size to be downloaded to each of Plaintiffs' iDevices and for purposes unrelated to those expected in the Weather Channel App." *Id.* Additionally, the transmission of personal information to the Mobile Industry Defendants was done without encryption, thus "exposing each Plaintiff to unreasonable risks of the interception of their personal information." *Id.* ¶¶ 66–67. Finally, Plaintiffs allege that as a result of Apple's failure to disclose its practices with respect to the allegedly "free apps," Plaintiffs overpaid for their iDevices. In other words "[h]ad Apple disclosed the true cost of the purportedly free Apps ... the value of the iPhones would have been materially less than what Plaintiffs paid."*Id.* ¶ 29.

The Geolocation Class

Additionally, Plaintiffs Gupta and Rodimer represent the "Geolocation Class," a putative class of iDevice purchasers who "have unwittingly, and without notice or consent transmitted location data to Apple's servers." *Id.* ¶ 204. Apple designed its iOS 4 software to retrieve and transmit geolocation information located on its customers' iPhones to Apple's servers. *Id.* ¶ 30. Plaintiffs

allege that in June 2010, with the release of its iOS 4 operating system, Apple began intentionally collecting Plaintiffs' precise geographic location and storing that information on the iDevice in order to develop an expansive database of information about the geographic location of cellular towers and wireless networks throughout the United States. *Id.* ¶¶ 115, 137. The geographic location information was accumulated from either Wi-fi towers or cell phone towers, and in some cases from the GPS data on Plaintiffs' devices. *Id.* ¶ 115. Apple represented that users could prevent Apple from collecting geolocation data about them by switching the Location Services setting on their iDevices to "off." *Id.* ¶ 31. Plaintiffs contend that Apple continued to monitor and store information about Plaintiffs locations even when the functionality was disabled ***1051*** on users' iDevices. *Id.* ¶¶ 32, 141. Plaintiffs contend that had Apple "disclosed the true cost of the ... geolocation features, the value of the iPhones would have been materially less than what Plaintiffs paid." *Id.* ¶ 29. Moreover, Plaintiffs allege that the storage of the location histories on their iDevices consume valuable memory space. *Id.* ¶ 119–121.

B. Procedural History

This case is a consolidated multi-district litigation involving nineteen putative class action lawsuits. *See generally* First Consolidated Class Action Complaint ("Consolidated Complaint"), 10–cv–05878–LHK, ECF No. 71. The first two of these consolidated actions were filed on December 23, 2010. *See Lalo v. Apple, Inc.*, et al., 10–cv–05878–LHK (the "Lalo Action") and *Freeman v. Apple, Inc., et al.*, 10–cv–05881–LHK (the "Freeman Action"). Other actions in this District and throughout the country have followed. These other actions, filed throughout the country, involve substantially similar allegations against Apple and other Defendants. On August 25, 2011, the Judicial Panel on Multidistrict Litigation ("MDL Panel") issued a Transfer Order, centralizing these actions in the Northern District of California before the undersigned. *See* August 25, 2011 Transfer Order in MDL No. 2250, ECF No. 1.
…

III. ANALYSIS

A. Article III Standing

An Article III federal court must ask whether a plaintiff has suffered sufficient injury to satisfy the "case or controversy" requirement of Article III of the U.S. Constitution. To satisfy Article III standing, plaintiff must allege: (1) injury-in-fact that is concrete and particularized, as well as actual and imminent; (2) wherein injury is fairly traceable to the challenged action of the defendant; and (3) it is likely (not merely speculative) that injury will be redressed by a favorable decision. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180–81, 120 S.Ct. 693, 145 L.Ed.2d 610 (2000); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561–62, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992). A suit brought by a plaintiff without Article III standing is not a "case or controversy," and an Article III federal court therefore lacks subject matter jurisdiction over the suit. *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 101, 118 S.Ct. 1003, 140 L.Ed.2d 210 (1998). In that event, the suit should be dismissed under Rule 12(b)(1). *See id.* at 109–110, 118 S.Ct. 1003.

Because “injury” is a requirement under both Article III and Plaintiffs' individual causes of action, the Court notes at the outset that “the threshold question of whether [Plaintiffs have] standing (and the ***1054*** [C]ourt has jurisdiction) is distinct from the merits of [Plaintiffs'] claim.”*Maya v. Centex Corp.*, 658 F.3d 1060, 1068 (9th Cir.2011). Standing “in no way depends on the merits of the plaintiff's contention that particular conduct is illegal.” *Warth*, 422 U.S. at 500, 95 S.Ct. 2197; *accord Equity Lifestyle Props., Inc. v. Cnty. of San Luis Obispo*, 548 F.3d 1184, 1189 n. 10 (9th Cir.2008) (“The jurisdictional question of standing precedes, and does not require, analysis of the merits.”). In other words “[a] plaintiff may satisfy the injury-in-fact requirements to have standing under Article III, and thus may be able to ‘bring a civil action without suffering dismissal for want of standing to sue,’ without being able to assert a cause of action successfully.” *In re Facebook Privacy Litig.*, 791 F.Supp.2d 705, 712 n. 5 (N.D.Cal.2011) (citing *Doe v. Chao*, 540 U.S. 614, 624–25, 124 S.Ct. 1204, 157 L.Ed.2d 1122 (2004)). Defendants argued in their briefing and at the hearing that Plaintiffs continue to rely on a faulty theory of injury and thus have failed to establish injury in fact that is fairly traceable to the Defendants such that Article III standing has been established. The Court disagrees.

1. Injury In Fact

Plaintiffs' initial complaint relied heavily upon a theory that collection of personal information itself created a particularized injury for the purposes of Article III standing. Relying on *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *3–5, 2011 U.S. Dist. LEXIS 50543, at *7–13 (C.D.Cal. Apr. 28, 2011), *In re DoubleClick, Inc., Privacy Litig.*, 154 F.Supp.2d 497, 525 (S.D.N.Y.2001), and *In re JetBlue Airways Corp., Privacy Litig.*, 379 F.Supp.2d 299, 327 (E.D.N.Y.2005), the Court found that Plaintiffs had “not identified an actual injury to themselves,” and that “any amended complaint must provide specific allegations with respect to the causal connection between the exact harm alleged (whatever it is) and each Defendants' conduct or role in that harm.” September 20 Order at 7 & 9. Additionally, the Court identified the following deficiencies in Plaintiffs' original complaint with respect to the threshold inquiry regarding whether Plaintiffs have established Article III standing: (a) which “iDevices they used;” (b) “which Defendant (if any) accessed or tracked their personal information;” (c) which apps they downloaded that “access[ed]/track[ed] their personal information,” and; (d) “what harm (if any) resulted from the access or tracking of their personal information.” September 20 Order at 6.

In contrast to the First Consolidated Complaint, Plaintiffs' allegations in the Amended Consolidated Complaint have been significantly developed to allege particularized injury to the Plaintiffs in this case. For one, Plaintiffs have articulated additional theories of harm beyond their theoretical allegations that personal information has independent economic value. In particular, Plaintiffs have alleged actual injury, including: diminished and consumed iDevice resources, such as storage, battery life, and bandwidth (AC ¶¶ 3, 63b, 72d, 198); increased, unexpected, and unreasonable risk to the security of sensitive personal information (AC ¶¶ 4, 18, 66–67); and detrimental reliance on Apple's representations regarding the privacy protection afforded to users of iDevice apps (AC ¶¶ 72c, 80–82).

Additionally, Plaintiffs have addressed the deficiencies identified in the Court's September 20 Order. Specifically, in the Amended Consolidated Complaint, Plaintiffs describe: (a) the specific

iDevices used (*see, e.g.,* AC ¶¶ 64a-g); (b) which Defendants accessed or tracked their personal information (*see, e.g.,* AC ¶¶ 56–63); (c) which apps they downloaded that accessed or tracked their personal information ***1055** (*see, e.g.,* AC ¶¶ 58–60); and (d) what harm resulted from the access or tracking of their personal information (*see, e.g.,* AC ¶¶ 3–4, 18, 63b, 66–67, 72d, 80–82, 198). Plaintiffs have also identified the specific type of personal information collected, such as Plaintiffs' home and workplace locations, gender, age, zip code, terms searched, Plaintiff's app ID and password for specific app accounts, etc., through each of the downloaded apps. *See, e.g.,*AC ¶¶ 58–64. Thus, Plaintiffs have addressed the concerns identified in the Court's September 20 Order and have articulated a particularized harm as to themselves.

…

[T]he Court finds that Plaintiffs have established injury in fact for the purposes of Article III standing.

…

B. Rule 12(b)(6) Motion to Dismiss Causes of Action

In light of the Court's finding that Plaintiffs have established Article III standing, the Court will turn to whether Plaintiffs have plausibly stated a claim as to each cause of action alleged in the Amended Consolidated Complaint.

1. Stored Communications Act

Plaintiffs' first claim, brought by Plaintiffs Gupta and Rodimer on behalf of the Geolocation Class solely against Apple, is that Apple's conduct violated the federal Stored Communications Act, 18 U.S.C. § 2701, et seq. ("SCA"). AC ¶¶ 224–25. Plaintiffs bring a separate claim under the SCA on behalf of the iDevice Class against all Mobile Industry Defendants.[4] AC ¶ 347. Enacted in 1986 as Section II of the Electronic Communications Protection Act ("ECPA"), the SCA creates criminal and ***1057** civil liability for certain unauthorized access to stored communications and records. *See Konop v. Hawaiian Airlines, Inc.,* 302 F.3d 868, 874 (9th Cir.2002). The SCA creates a private right of action against anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a); see id. § 2707 (creating a private right of action). The general prohibitions under § 2701(a), however, do not apply "to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c).

Plaintiffs Gupta and Rodimer assert that Apple violated § 2701(a)(1) and (a)(2) by intentionally accessing and collecting temporarily stored location data from Geolocation Class members' iPhones after Locations Services was turned "off." AC ¶¶ 224–25. Plaintiffs further assert that the Mobile Industry Defendants violated § 2701(a)(1) by intentionally accessing electronic communications while in electronic storage by collecting temporarily stored location data from the iDevice Class's iPhones. *See* AC ¶¶ 58–64, 347.

Both Apple and the Mobile Industry Defendants advance four arguments why Plaintiffs' SCA claims should be dismissed for failure to state a claim, which the Court will address in turn: (1) an iPhone is not a "facility through which an electronic communication service is provided;" (2) location data on users' iPhones is not in "electronic storage;" (3) Defendants are either the electronic communications services ("ECS") providers or the intended recipient of the communications, so Plaintiffs' claims are barred by the exceptions contained in 18 U.S.C. § 2701(c)(1)-(2); and (4) Plaintiffs allege only that the iPhones communicated with Apple's servers, not that Apple accessed Plaintiffs' iPhones through unauthorized log-ins.

a. Facility

To state a claim under the SCA, Plaintiffs must allege that Defendants accessed without authorization "a facility through which an electronic communication service is provided." 18 U.S.C. § 2701(a)(1). An "electronic communication service" ("ECS") is "any service which provides to users thereof the ability to send and receive wire or electronic communications." 18 U.S.C. § 2510(15). While the computer systems of an email provider, a bulletin board system, or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users, less consensus surrounds the question presented here: whether an individual's computer, laptop, or mobile device fits the statutory definition of a "facility through which an electronic communication service is provided." The Court agrees with Defendants that it does not. Plaintiffs do not suggest that something other than their iPhones are the "facilities" allegedly accessed without authorization. *See generally* Opp'n at 10–11. Instead, Plaintiffs urge the Court to follow a number of non-binding decisions that have accepted that personal computers can be facilities.

…

[T]he courts that have taken a closer analytical look have consistently concluded that an individual's personal computer does not "provide [ ] an electronic communication service" simply by virtue of enabling use of electronic communication services. *See, e.g., Crowley v. CyberSource Corp.*, 166 F.Supp.2d 1263, 1270–71 (N.D.Cal.2001). In *Crowley*, the plaintiff made a similar argument that "computers of users of electronic communication service, as opposed to providers of electronic communication service, are considered facilities through which such service is provided." 166 F.Supp.2d at 1271. The *Crowley* court rejected the argument that a user's computer is a "facility" under the SCA, because adopting plaintiff's construction would render other parts of the statute illogical. Another provision of the statute authorizes access to a "facility" by a provider of an electronic communication service. 18 U.S.C. § 2701(c)(1). Following Plaintiffs' logic, a service provider could grant access to a user's computer (the "facility"). "It would certainly seem odd that the provider of a communication service could grant access to one's home computer to third parties, but that would be the result of [plaintiff's] argument." *Id.*(citing 18 U.S.C. § 2701(c)(1)).

…

b. Electronic Storage

Next, Defendants argue that information stored on a user's iPhone cannot be information in "electronic storage" for purposes of the SCA. To state a claim under the SCA, Plaintiffs must show not only that Defendants accessed a facility through which an electronic communication service is provided, but furthermore that Defendants "obtain[ed], alter[ed], or prevent[ed]

authorized access to a wire or electronic communication while it [was] in electronic storage in such system." 18 U.S.C. § 2701(a) (emphasis added). The SCA defines "electronic storage" as "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) ***1059** any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

The Court finds persuasive the reasoning in *In re DoubleClick, Inc. Privacy Litigation,* 154 F.Supp.2d 497 (S.D.N.Y.2001). There, the court dismissed an SCA claim upon finding that the identification numbers for browser cookies the defendants installed on the plaintiffs' computers were not in "electronic storage" because they resided on the plaintiff's hard drives and thus were not in temporary electronic storage, as is required by the Act. In *In re DoubleClick,* the district court, after considering the plain language of the statute, concluded that "[the SCA] only protects electronic communications stored 'for a limited time' in the 'middle' of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it."154 F.Supp.2d at 512 (quoting dictionary definitions of "temporary" and "intermediate"). The district court concluded that "[t]he cookies' long-term residence on plaintiffs' hard drives places them outside of § 2510(17)'s definition of 'electronic storage' and, hence, Title II [of the ECPA's] protection." *Id.* at 511.

…

Here, the Geolocation Plaintiffs allege that Apple retrieved information from their iPhones revealing their real-time location information and that this information was necessarily only "temporarily stored" on their iPhones, because "anything other than temporary and regularly overwritten ... data (constantly updated cell tower and WiFi network information) would quickly consume the iPhone's available memory." Opp'n at 11–12. However, Plaintiffs' own allegations in the amended complaint state that "in the /Library/Application Support/MobileSync/Backups/ folder on a user's iDevice, Apple maintains an unencrypted log of the user's movements, as often as 100 times a day, for up to a one-year period." AC ¶ 107(a). Thus, it appears that this location data resides on Plaintiffs' iPhone hard drive for up to a one-year period, which is not merely a "temporary, intermediate storage ... incidental to the electronic transmission" of an electronic communication. Nor do Plaintiffs allege that Defendants accessed the data at a time when the data was only in temporary, intermediate storage. Thus, the Court again agrees with Defendants that Plaintiffs fail to state a claim under the SCA because they fail to allege that Defendants accessed data in "electronic storage."

c. Statutory Exceptions

Defendants argue that, even if Plaintiffs had alleged that Apple accessed a communication in "electronic storage" in a "communications facility," this conduct would fall under specific SCA exceptions for service providers or intended parties to certain communications, as provided by § 2701(c)(2). Under § 2701(c), conduct authorized by the ECS provider falls beyond the scope of § 2701(a)(1). Likewise, ***1060** § 2701(a) does not apply with respect to conduct authorized "by a user of that [electronic communications] service with respect to a communication of or intended for that user." *See* 18 U.S.C. § 2701(c).

The Court finds that the second exception under § 2701(c) applies to the Mobile Industry Defendants, but not to Apple. Here, Plaintiffs allege that Apple itself caused a log of geolocation data to be generated and stored, and that Apple designed the iPhone to collect and send this data to Apple's servers. AC ¶¶ 107(a), 114, 138. Apple, however, is neither an electronic communications service provider, nor is it a party to the electronic communication between a user's iPhone and a cellular tower or WiFi tower. Thus, the Court fails to see how Apple can avail itself of the statutory exception by creating its own, secondary communication with the iPhone. With respect to the Mobile Industry Defendants, Plaintiffs allege that when users download and install Apps on their iPhones, the Mobile Industry Defendants' software accesses personal information on those devices and sends that information to Defendants. AC ¶ 161. These allegations are highly similar to those dismissed in *In re DoubleClick* and *In re Facebook Privacy Litigation,* 791 F.Supp.2d 705 (N.D.Cal.2011) (Ware, J.). Thus, the App providers are akin to the web sites deemed to be "users" in *In re DoubleClick,* and the communications at issue were sent to the App providers. *See* 154 F.Supp.2d at 508–09. Thus, because the communications were directed at the App providers, the App providers were authorized to disclose the contents of those communications to the Mobile Industry Defendants. The Mobile Industry Defendants' actions therefore fall within the statutory exception of the SCA.

d. Access Without Authorization

Defendants' final argument is that Plaintiffs fail to state a claim under the SCA because they have not alleged that Defendants "accessed" their iPhones, even if their iPhones are considered "facilities" under the SCA. Defendants again cite the *Crowley* decision, where the district court found that, notwithstanding plaintiff's conclusory allegations that the defendants "accessed" his computer, in fact "Crowley sent his information to Amazon electronically; Amazon did not gain access to his computer in order to obtain the personal information at issue." *Crowley,* 166 F.Supp.2d at 1271.

The reasoning in *Crowley* is not as applicable to this particular argument because the nature of Plaintiffs' allegations here is rather distinct. Plaintiffs allege that when users download and install Apps on their iPhones, the Mobile Industry Defendants' software accesses personal information on those devices and supplies Defendants with details such as consumers' cellphone numbers, address books, UDIDs, and geolocation histories. AC ¶ 161. This information is not simply information that Plaintiffs themselves have voluntarily sent to the App developers, but rather information that is stored on the iPhone.

Although the Court is not persuaded that Plaintiffs have failed to allege that Defendants "accessed" their iPhones in order to obtain location data, the Court concludes that Plaintiffs have failed to allege facts sufficient to support a claim that Defendants accessed a communications facility and thereby obtained access to an electronic communication while it was in electronic storage in such system. Accordingly, Defendants' respective motions to dismiss claims one and eleven for violations of the SCA are GRANTED. The motions are granted with prejudice, for the reasons discussed in Section III.D.

***1061* 2. Wiretap Act**

Plaintiffs' second claim, brought by Plaintiffs Gupta and Rodimer on behalf of the Geolocation Class solely against Apple, is that Apple's conduct violated two provisions of the federal Wiretap Act, 18 U.S.C. §§ 2510–2522 (2000). *See* AC ¶¶ 230–31. The Wiretap Act generally prohibits the "interception" of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1). More specifically, the Wiretap Act provides a private right of action against any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," 18 U.S.C. § 2511(1)(a), or who "intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [the Wiretap Act]," *id.* § 2511(1)(d). *See id.* § 2520 (providing a private right of action). Plaintiffs here assert that Apple violated § 2511(1)(a) and § 2511(1)(d) by collecting Plaintiffs' precise geographic location data from Wi-fi towers, cell phone towers, and GPS data on Plaintiffs' devices, and by using that location data to develop an expansive database of information about the geographic location of cellular towers and wireless networks throughout the United States, to Apple's benefit. AC ¶¶ 115, 137, 230–31.

Apple contends that Plaintiffs have failed to state a claim under the Wiretap Act for the following two reasons: (1) location data is not the "content" of any communication for purposes of the Wiretap Act; and (2) Apple could not have unlawfully "intercepted" the communication because it was the intended recipient of the location data. Apple MTD at 20–22.

a. Content of Communications

The Wiretap Act prohibits "interceptions" of electronic communications and defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." § 2510(4) (emphasis added). The "contents" of a communication, in turn, are defined in the statute as "any information concerning the substance, purport, or meaning of that communication." § 2510(8). "[A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce," with certain exceptions not relevant to this case, qualifies as an "electronic communication." § 2510(12).

Apple argues that information about the identities of parties to a communication and other call data is not "content" as defined by the Wiretap Act. The Court agrees. In *United States v. Reed*, 575 F.3d 900 (9th Cir.2009), the Ninth Circuit held that data automatically generated about a telephone call, such as the call's time of origination and its duration, do not constitute "content" for purposes of the Wiretap Act's sealing provisions because such data "contains no 'information concerning the substance, purport, or meaning of [the] communication.' " *Id.* at 916 (quoting 18 U.S.C. § 2510(5)). Rather, "content" is limited to information the user intended to communicate, such as the words spoken in a phone call. *Id.* Here, the allegedly intercepted electronic communications are simply users' geolocation data. This data is generated automatically, rather than through the intent of the user, and therefore does not constitute "content" susceptible to interception.

1062 Plaintiffs cite *In re Pharmatrak, Inc.*, 329 F.3d 9 (1st Cir.2003), for the proposition that the definition of "contents" "encompasses personally identifiable information." Opp'n to Apple MTD at 15 (quoting *In re Pharmatrak,* 329 F.3d at 18). The Court does not find *In re Pharmatrak* persuasive because *In re Pharmatrak* cites to a footnote of a 1972 Supreme Court case discussing an outdated version of the Wiretap Act. *See Gelbard v. United States*, 408 U.S. 41, 51 n. 10, 92 S.Ct. 2357, 33 L.Ed.2d 179 (1972). The version of the Wiretap Act discussed in*Gelbard* defined "contents" as including "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (1972). The pre–1986 definition "incude[s] all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded." *Gelbard*, 408 U.S. at 51 n. 10, 92 S.Ct. 2357 (quoting S.Rep. No. 1097; internal quotation marks omitted). Congress, however, amended this definition in 1986 by specifically excising the phrase "information concerning the identity of the parties to such communication or the existence ... of that communication." *See* § 2510(8) (1986). Thus, the Court concludes that under the current version of the statute, personally identifiable information that is automatically generated by the communication but that does not comprise the substance, purport, or meaning of that communication is not covered by the Wiretap Act. Because Plaintiffs allege the interception only of automatically generated geolocation data, Plaintiffs have not stated a claim for relief under the federal Wiretap Act.

b. Interception

The Court is less convinced by Apple's second argument that dismissal is warranted because Apple was the intended recipient of the Geolocation Class members' location data and therefore cannot be held liable under the Wiretap Act. Apple invokes a statutory exception to liability that protects the intended recipient of a communication. The exception provides that it is not "unlawful ... for a person not acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or [any federal or state law]." 18 U.S.C. § 2511(2)(d).

Apple points to the assertion in the AC that "Apple designed iOS 4 to access and transmit location data from the mobile device to Apple's servers," and from that statement concludes that Apple is an intended recipient of the location data from users' mobile devices. *See* AC ¶ 142. However, this is not a fair reading of the Plaintiffs' allegations. The intended communication is between the users' iPhone and the Wi-fi and cell phone towers, and Plaintiffs appear to allege that Apple designed its operating system to intercept that communication and transmit the information to Apple's servers. Apple cannot manufacture a statutory exception through its own accused conduct, and thus the Court does not agree that § 2511(2)(d) applies.

In sum, Plaintiffs have failed to state a claim under § 2511(1)(a) or § 2511(1)(d). Accordingly, Apple's motion to dismiss count two for violation of the Wiretap Act is GRANTED. The motion is granted with prejudice, for the reasons discussed in Section III.D.

***1063* 3. Invasion of Privacy Under the California Constitution**

Plaintiffs, on behalf of both the Geolocation and iDevice Classes, assert that Defendants' conduct violates their right to privacy pursuant to Article I, Section 1 of the California Constitution. The California Constitution creates a privacy right that protects individuals from the invasion of their privacy not only by state actors but also by private parties. *Am. Acad. of Pediatrics v. Lungren*, 16 Cal.4th 307, 66 Cal.Rptr.2d 210, 940 P.2d 797 (1997); *Leonel v. Am. Airlines, Inc.*, 400 F.3d 702, 711–12 (9th Cir.2005), *opinion amended on denial of reh'g*, 03–15890, 2005 WL 976985 (9th Cir. Apr. 28, 2005). To prove a claim under the California Constitutional right to privacy, a plaintiff must first demonstrate three elements: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest.*Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal.4th 1, 35–37, 26 Cal.Rptr.2d 834, 865 P.2d 633 (1994). These elements do not constitute a categorical test, but rather serve as threshold components of a valid claim to be used to "weed out claims that involve so insignificant or de minimis an intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant." *Loder v. City of Glendale*, 14 Cal.4th 846, 59 Cal.Rptr.2d 696, 927 P.2d 1200 (1997).

Even assuming, without deciding, that Plaintiffs have established the first two elements of a constitutional invasion of privacy claim, Plaintiffs' claim fails under the third element. "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an *egregious breach* of the social norms underlying the privacy right." *Hill*, 7 Cal.4th 1, 26, 37, 26 Cal.Rptr.2d 834, 865 P.2d 633 (1994) (holding that rules requiring college football players to submit to drug testing were not egregious breaches of the social norms) (emphasis added). Even negligent conduct that leads to theft of highly personal information, including social security numbers, does not "approach [the] standard" of actionable conduct under the California Constitution and thus does not constitute a violation of Plaintiffs' right to privacy. *See Ruiz v. Gap, Inc.*, 540 F.Supp.2d 1121, 1127–28 (N.D.Cal.2008) *aff'd*, 380 Fed.Appx. 689 (9th Cir.2010).

Here, the information allegedly disclosed to third parties included the unique device identifier number, personal data, and geolocation information from Plaintiffs' iDevices. Even assuming this information was transmitted without Plaintiffs' knowledge and consent, a fact disputed by Defendants, such disclosure does not constitute an egregious breach of social norms. *See, e.g. Folgelstrom v. Lamps Plus, Inc.*, 195 Cal.App.4th 986, 992, 125 Cal.Rptr.3d 260 (2011) ("Here, the supposed invasion of privacy essentially consisted of [Defendant] obtaining plaintiff's address without his knowledge or permission, and using it to mail him coupons and other advertisements. This conduct is not an egregious breach of social norms, but routine commercial behavior."). Accordingly, Plaintiffs have failed to establish that Defendants' conduct "amounts to a serious invasion" of the protected privacy interest. *See Hill*, 7 Cal.4th at 26, 26 Cal.Rptr.2d 834, 865 P.2d 633. Therefore, Defendants' motions to dismiss counts three and four for violations of California's constitutional right to privacy are GRANTED. …
…

The Geolocation Class

Plaintiffs, on behalf of the Geolocation Class, assert that Apple's practice of using iDevices to retain location history files violates the above referenced provisions of the CFAA. Apple[5] first argues that Plaintiffs ***1066*** have failed to state a claim pursuant to the CFAA because Plaintiffs have not pled facts that establish that Apple accessed the iOS Devices without authorization. The Court agrees.

Apple rightly argues that class members "voluntarily installed" the software that caused users' iDevices to maintain, synchronize, and retain detailed, unencrypted location history files.AC ¶ 264; Apple's Mot. to Dismiss at 23. Voluntary installation of software that allegedly harmed the phone was *voluntarily downloaded* by the user. Other courts in this District and elsewhere have reasoned that users would have serious difficulty pleading a CFAA violation. *See In re Apple & ATTM Antitrust Litig.*, 2010 WL 3521965, at *7, 2010 U.S. Dist. LEXIS 98270, at *26 (N.D.Cal. July 8, 2010) ("Voluntary installation runs counter to the notion that the alleged act was a trespass and to CFAA's requirement that the alleged act was 'without authorization' as well as the CPC's requirement that the act was 'without permission.' "); *see also Specific Media*, 2011 WL 1661532, at *6, 2011 U.S. Dist. LEXIS 50543, at *18 (on factual allegations similar to those here, noting that "it is unclear whether Specific Media can be said to have 'intentionally caus[ed] damage' to Plaintiffs' computers."). Although Apple arguably exceeded its authority when it continued to collect geolocation data from Plaintiffs after Plaintiffs had switched the Location Services setting to "off," Plaintiffs are not asserting an "exceeds authorized access" claim against Apple. Instead, Apple had authority to access the iDevice and to collect geolocation data as a result of the voluntary installation of the software (either as an update or as a native installation).

Additionally, Apple argues that the type of harm alleged with respect to this class—the cost of memory space on the class members' iPhones as a result of storing unauthorized geolocation data—is insufficient to establish the $5,000 damages minimum. In order to establish access and transmission claims pursuant to the CFAA, as the Geolocation Class attempts to here, Plaintiffs must establish that they suffered economic damage. *See Czech v. Wall Street on Demand, Inc.*,674 F.Supp.2d 1102, 1110 (D.Minn.2009). A plaintiff may aggregate individual damages over the putative class to meet the damages threshold if the violation can be described as "one act." *In re Toys R Us, Inc. Privacy Litig.*, 2001 WL 34517252, *11 (N.D.Cal.2001); *see also Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir.2004); *see In re DoubleClick Privacy Litig.*, 154 F.Supp.2d 497, 523 (S.D.N.Y.2001).

Here, although Plaintiffs allege that the storage of the location histories on their iDevices consume valuable memory space, which constitutes economic damages for the purposes of the CFAA, courts have consistently rejected this argument in similar contexts. *See, e.g. Del Vecchio v. Amazon.com, Inc.*, C11–366, 2011 WL 6325910, at *4 (W.D.Wa. Dec. 1, 2011) ("concluding that Plaintiffs failed to establish the $5,000 minimum damages under the CFAA where Plaintiffs had not alleged that he or she discerned any difference whatsoever in the performance of his or her computer while visiting Defendants' site, let alone any diminution from which ***1067*** the Court could plausibly infer the necessary damages."); *Bose v. Interclick, Inc.*, No. 10 Civ. 9183(DAB), 2011 WL 4343517, at *4, 2011 U.S. Dist. LEXIS 93663, at *12–14 (S.D.N.Y. Aug. 17, 2011)(finding that Plaintiff failed to establish the economic injury required by the CFAA even though Plaintiff alleged that Defendant "impaired the functioning and diminished the value

of Bose's computer in a general fashion"); *Fink v. Time Warner Cable*, No. 08 Civ. 9628, 2009 WL 2207920, *4 (S.D.N.Y. July 23, 2009) (dismissing a CFAA claim because Plaintiff only alleged that Defendant caused damage by impairing the integrity or availability of data and information, which was insufficiently factual to frame plausibly the damages element of Plaintiff's CFAA claim).

Typically, in order to establish economic damages, the consumer must establish that the Defendant intended to impair the recipient's service. *Czech*, 674 F.Supp.2d at 1115. For example, a Defendant's unwanted text messages, alone do not cause "damage" to a consumer's cell phone by consuming limited resources. *Id.* (although the CFAA recognizes no de minimis or nominal damage exception, "the question remains whether Czech's allegations establish that her receipt of unwanted text messages necessarily constitutes 'impairment' of any magnitude."). Damage under the CFAA does not occur simply by "any use or consumption of a device's limited resources," but rather "damage" must arise from an impairment of performance "that occurs when the cumulative impact of all calls or messages at any given time exceeds the device's finite capacity so as to result in a slowdown, if not an outright 'shutdown,' of service." *Id.* at 1117; *cf.America Online, Inc. v. Nat'l Health Care Discount, Incorp.*, 121 F.Supp.2d 1255, 1274 (N.D.Iowa 2000) ("when a large volume of [spam] causes slowdowns or diminishes the capacity of AOL to service its customers, an 'impairment' has occurred to the 'availability' of AOL's system.").

The Court further finds persuasive the reasoning employed in *AtPac, Inc. v. Aptitude Solutions, Inc.*, in which the district court narrowly construed the class of cases in which civil actions may be brought pursuant to the CFAA:

> Congress' restricting of civil actions to cases that cause the types of harm listed in18 U.S.C. § 1030(c)(4)(A)(i) subsections (I) through (V) reemphasizes the court's conclusion that the sort of conduct alleged against [defendant] does not fall under the CFAA's prohibitions. "Loss" is grouped along with the harms of physical injury, threat to public health and safety, impairment of medical diagnosis or treatment, and damage to federal government computers that deal with national security and defense. It is no surprise that courts interpreting the definition of "loss" sufficient to bring a civil action have done so narrowly given the company that subsection (I) keeps. The definition of "loss" itself makes clear Congress's intent to restrict civil actions under subsection (I) to the traditional computer "hacker" scenario-where the hacker deletes information, infects computers, or crashes networks.

730 F.Supp.2d at 1185.

Although Plaintiffs have alleged that the location files consume valuable memory space on their iDevices, Plaintiffs have not plausibly alleged that the location file *impairs* Plaintiffs' devices or interrupts service, or otherwise fits within the statutory requirements of "loss" and "economic damage" as defined by the statute. 18 U.S.C. § 1030(e)(11), (8). Thus, the Geolocation Class has failed to state a claim under the CFAA.

The iDevice Class

The Plaintiffs' claim under the CFAA on behalf of the iDevice Class suffers from a ***1068*** similar defect as the claims on behalf of the Geolocation Class. As the Court recognized in theSeptember 20 Order, Plaintiffs have failed to sufficiently allege that Defendants accessed Plaintiffs' iDevices "without authorization." Where, as here, the software or "apps" that allegedly harmed the phone were voluntarily downloaded by the user, other courts in this District and elsewhere have reasoned that users would have serious difficulty pleading a CFAA violation. *SeeIn re Apple & ATTM Antitrust Litig.,* 2010 WL 3521965, at *7, 2010 U.S. Dist. LEXIS 98270, at *26 (N.D.Cal. July 8, 2010) ("Voluntary installation runs counter to the notion that the alleged act was a trespass and to CFAA's requirement that the alleged act was 'without authorization' as well as the CPC's requirement that the act was 'without permission.' "); *see also Specific Media,* 2011 WL 1661532, at *6, 2011 U.S. Dist. LEXIS 50543, at *18 (on factual allegations similar to those here, noting that "it is unclear whether Specific Media can be said to have 'intentionally caus[ed] damage' to Plaintiffs' computers.").

Moreover, Plaintiffs have not established that the alleged privacy breaches performed by the Mobile Industry Defendants and allowed by Apple meet the statutory loss required for all civil actions identified above. Plaintiffs have put forth two theories that they believe demonstrate "loss to 1 or more persons during any 1–year period ... aggregating at least $5,000" in "economic damages." *Id.* at § 1030(g) & (c)(4)(A)(i)(I)(V). As explained below, both of these theories are insufficient to establish civil liability under the CFAA.

As explained previously in the September 20 Order, courts have tended to reject the contention that personal information—such as the information collected by the Mobile Industry Defendants—constitutes economic damages under the CFAA. *See, e.g. In re Zynga Privacy Litig.,* 2011 WL 7479170, at *3 (N.D.Cal. June 15, 2011) (rejecting the allegation that Plaintiffs' personally identifiable information constitutes a form of money or property, such that Defendant's alleged misappropriation and disclosure of that information would constitute "damage or loss ... in excess of $5,000."); *Del Vecchio,* 2011 WL 6325910, at *3 ("While it may be theoretically possible that Plaintiffs' information could lose value as a result of its collection and use by Defendant, Plaintiffs do not plead any facts from which the Court can reasonably infer that such devaluation occurred in this case."); *Bose,* 2011 WL 4343517, at *4 ("Only economic damages or loss can be used to meet the $5,000 threshold" and "[t]he collection of demographic information does not constitute damage to consumers or unjust enrichment to collectors.") (internal citation marks omitted).

Similarly, while Plaintiffs allege that the creation of location history files and app software components "consumed portions of the cache and/or gigabytes of memory on their devices." AC ¶ 72(d), and that the Mobile Industry Defendants conduct shortens the battery life of the iDevice, these allegations do not plausibly establish that Defendant's conduct impairs Plaintiffs' devices or service. *See, e.g. Czech,* 674 F.Supp.2d at 1117 (rejecting CFAA under similar allegations of "impairment" to plaintiff's phone because the damage does not occur simply by "any use or consumption of a device's limited resources," but rather "damage" must arise from an impairment of performance "that occurs when the cumulative impact of all calls or messages at any given time exceeds the device's finite capacity so as to result in a slowdown, if not an outright 'shutdown,' of service."); *cf. America Online, Inc. v. Nat'l Health Care Discount,*

Incorp., 121 F.Supp.2d 1255, 1274 (N.D.Iowa 2000) ("when a large volume of ***1069*** [spam] causes slowdowns or diminishes the capacity of AOL to service its customers, an 'impairment' has occurred to the 'availability' of AOL's system."). Thus, the iDevice Class Plaintiffs have also failed to allege actionable damages pursuant to the CFAA.

In sum, Defendants' motions to dismiss the sixth and seventh causes of action for violations of the CFAA are GRANTED. The motions are granted with prejudice, for the reasons set forth in Section III.D.

6. Trespass

Plaintiffs, on behalf of both the Geolocation and iDevice Classes, assert a claim for trespass against all Defendants. Under California law, trespass to chattels "lies where an intentional interference with the possession of personal property has proximately caused injury." *Intel Corp. v. Hamidi*, 30 Cal.4th 1342, 1350–51, 1 Cal.Rptr.3d 32, 71 P.3d 296 (2003). In cases of interference with possession of personal property not amounting to conversion, "the owner has a cause of action for trespass or case [sic], and may recover only the actual damages suffered by reason of the impairment of the property or the loss of its use." *Id.* at 1351, 1 Cal.Rptr.3d 32, 71 P.3d 296 (internal quotations and citations omitted). "[W]hile a harmless use or touching of personal property may be a technical trespass (see Rest.2d Torts, § 217), an interference (not amounting to dispossession) is not *actionable*, under modern California and broader American law, without a showing of harm." *Id.* Even where injunctive relief is sought, "the plaintiff must ordinarily show that the defendant's wrongful acts threaten to cause *irreparable*injuries, ones that cannot be adequately compensated in damages." *Id.* at 1352, 1 Cal.Rptr.3d 32, 71 P.3d 296 (citing 5 Witkin, Cal. Procedure (4th ed.1997) Pleading, § 782, p. 239.).

An action for trespass arises "when [the trespass] actually did, or threatened to, interfere with the intended functioning of the system, as by *significantly reducing* its available memory and processing power." *Id.* at 1356, 1 Cal.Rptr.3d 32, 71 P.3d 296 (emphasis added). Similarly, "intermeddling is actionable only if 'the chattel is impaired as to its condition, quality, or value or ... the possessor is deprived of the use of the chattel for a substantial time.' " Plaintiffs, on behalf of the Geolocation Class, allege that Apple's creation of location history files and app software components "consumed portions of the cache and/or gigabytes of memory on their devices." Similarly, Plaintiffs, on behalf of the iDevice Class, allege that the apps provided by the Mobile Industry Defendants have taken up valuable bandwidth and storage space on their iDevices and Defendants' conduct has subsequently shortened the battery life of the iDevice. While these allegations conceivably constitute a harm, they do not plausibly establish a significant reduction in service constituting an interference with the intended functioning of the system, which is necessary to establish a cause of action for trespass. As *Hamidi* demonstrates, trespass without harm, "by reason of the impairment of the property or the loss of use," is not actionable. *Hamidi*, 30 Cal.4th at 1351, 1 Cal.Rptr.3d 32, 71 P.3d 296. Accordingly, Defendants' motions to dismiss Plaintiffs' eighth cause of action for trespass are GRANTED. …

…

9. Conversion

Plaintiffs, on behalf of the iDevice Class, allege that Apple and the Mobile Industry Defendants are liable for conversion. California law defines conversion as "any act of dominion wrongfully

asserted over another's personal property in denial of or inconsistent with his rights therein." *In re Bailey,* 197 F.3d 997, 1000 (9th Cir.1999). "The conversion of another's property without his knowledge or consent, done intentionally and without justification and excuse, to the other's injury, constitutes a willful and malicious injury within the meaning of § 523(a)(6)." *In re Bailey,* 197 F.3d at 1000 (citing *Transamerica Comm. Fin. Corp. v. Littleton,* 942 F.2d 551, 554 (9th Cir.1991)).

To establish conversion, a plaintiff must show "ownership or right to possession of property, wrongful disposition of the property right and damages." *Kremen v. Cohen,* 337 F.3d 1024, 1029 (9th Cir.2003). The court applies a three part test to determine whether a property right exists: "[f]irst, there must be an interest capable of precise definition; second, it must be capable of exclusive possession or control; and third, the putative owner must have established a legitimate claim to exclusivity." *Id.* at 1030; *Boon Rawd Trading Int'l Co. v. Paleewong Trading Co.,* 688 F.Supp.2d 940, 955 (N.D.Cal.2010).

****1075*** Plaintiffs again argue that their personal information is property which is capable of exclusive possession or control. The Court, in the September 20 Order, rejected a similar argument because the weight of authority holds that a plaintiff's "personal information" does not constitute property. *Thompson v. Home Depot, Inc.,* No. 07cv1058 IEG, 2007 WL 2746603, at *3 (S.D.Cal. Sept. 18, 2007); *In re Facebook Privacy Litig.,* 791 F.Supp.2d 705, 713–14 (N.D.Cal. May 12, 2011). Plaintiffs have also failed to establish that the broad category of information referred to as "personal information" is an interest capable of precise definition. "Personal information" includes such things as a user's location, zip code, device identifier, and other data. Moreover, it is difficult to see how this broad category of information is capable of exclusive possession or control. Therefore, Plaintiff's twelfth cause of action for conversion is DISMISSED. …

10. Unjust Enrichment/Assumpsit/Restitution

Plaintiffs, on behalf of the iDevice Class, allege a claim against Apple and the Mobile Industry Defendants for Assumpsit and Restitution. Notwithstanding earlier cases suggesting the existence of a separate, stand-alone cause of action for unjust enrichment, the California Court of Appeals has recently clarified that "[u]njust enrichment is not a cause of action, just a restitution claim." *Hill v. Roll Int'l Corp.,* 195 Cal.App.4th 1295, 1307, 128 Cal.Rptr.3d 109 (2011); *accord Levine v. Blue Shield of Cal.,* 189 Cal.App.4th 1117, 1138, 117 Cal.Rptr.3d 262 (2010); *Melchior v. New Line Prods., Inc.,* 106 Cal.App.4th 779, 793, 131 Cal.Rptr.2d 347 (2003); *Durell v. Sharp Healthcare,* 183 Cal.App.4th 1350, 1370, 108 Cal.Rptr.3d 682 (2010). In light of this recent persuasive authority, this Court has previously determined that "there is no cause of action for unjust enrichment under California law." *Fraley v. Facebook,* 830 F.Supp.2d 785, 814 (N.D.Cal.2011); *accord Ferrington v. McAfee, Inc.,* No. 10–cv–01455–LHK, 2010 WL 3910169, at *17 (N.D.Cal.2010). Other courts have similarly reached this conclusion. *See Robinson v. HSBC Bank USA,* 732 F.Supp.2d 976, 987 (N.D.Cal.2010) (Illston, J.) (dismissing with prejudice plaintiffs' unjust enrichment claim brought in connection with claims of misappropriation and violation of the UCL because unjust enrichment does not exist as a standalone cause of action);*LaCourt v. Specific Media, Inc.,* No. SACV 10–1256–GW(JCGx), 2011 WL 1661532 at *8 (C.D.Cal. Apr. 28, 2011) (dismissing unjust enrichment claim because it "cannot serve as an

independent cause of action"); *In re DirecTV Early Cancellation Litig.*, 738 F.Supp.2d 1062, 1091–92 (C.D.Cal.2010) (same). Thus, Plaintiffs' unjust enrichment claim does not properly state an independent cause of action and must be dismissed. *See Levine*, 189 Cal.App.4th at 1138, 117 Cal.Rptr.3d 262.

California courts have recognized multiple grounds for awarding restitution. *See McBride v. Boughton*, 123 Cal.App.4th 379, 389, 20 Cal.Rptr.3d 115 (2004) ("Under the law of restitution, an individual is required to make restitution if he or she is unjustly enriched at the expense of another."). Restitution may be awarded: "(1) in lieu of breach of contract damages when the parties had an express contract, but it was procured by fraud or is unenforceable or ineffective for some reason, or (2) when a Defendant obtained a benefit from the plaintiff by fraud, duress, conversion, or similar conduct." *Id.* at 388, 20 Cal.Rptr.3d 115. Thus, California law recognizes that a plaintiff may elect which remedy to seek: "the plaintiff may choose not to sue in tort, but instead to seek restitution ****1076*** on a quasi-contract theory (an election referred to at common law as 'waiving the tort and suing in assumpsit')." *Id.* (citing *Murrish v. Indust. Indem. Co.*, 178 Cal.App.3d 1206, 1209, 224 Cal.Rptr. 308 (1986)).

However, like unjust enrichment, California does not recognize a cause of action for restitution. *See Durell*, 183 Cal.App.4th at 1370, 108 Cal.Rptr.3d 682 (explaining that there is no cause of action in California for unjust enrichment and "[u]njust enrichment is synonymous with restitution."); *see also Robinson*, 732 F.Supp.2d at 987 ("There is no cause of action for restitution, but there are various causes of action that give rise to restitution as a remedy."). Thus, to the extent that Plaintiffs seek to assert restitution as a stand alone cause of action, Plaintiffs' claim is dismissed. To the extent that Plaintiffs seek to elect restitution as a remedy for another tort, Plaintiffs are not entitled to restitution because they have not stated a claim for common law tort such as conversion, nor has Plaintiff established that Defendants obtained a benefit from the plaintiff by fraud or duress separate and apart from the statutory claims discussed above. Accordingly, Defendants' motion to dismiss Plaintiffs' thirteenth cause of action is GRANTED.
…

C. User Agreements

Apple also argues that all of Plaintiffs' claims against it are foreclosed by Apple's Privacy Policy and the Terms and Conditions of the iTunes Apps Store (the "Agreement"). *See* Apple's Mot. to Dismiss at 11–14, McCabe Decl. Exs. F & G. Apple makes two main arguments: (1) to the extent that Plaintiffs contest Apple's collection and transfer of user data, Apple's conduct is explicitly permitted pursuant to the terms of the Privacy Policy, and (2) the iDevice Class's claims against Apple are foreclosed because the Agreement includes a disclaimer of liability arising from third party conduct.
…
Based on the record before the Court, Plaintiffs have a colorable argument that the terms of the privacy agreement were ambiguous and do not necessarily foreclose the remaining claims against Apple. ****1077*** On the one hand, the Agreement informs users that Apple may collect "non-personal information" including "zip code, area code, unique device identifier, [and] location" and the Agreement authorizes Apple to "collect, use, transfer, and disclose non-personal information for any purpose." However, Apple also limits how it may utilize users'

"personal information" which it defines as "data that can be used to uniquely identify or contact a single person." It does appear that there is some ambiguity as to whether the information collected by Apple, including the user's unique device identifier, is personal information under the terms of the Agreement, and thus whether Apple's collection and use of the information is consistent with the Agreement's terms.

Additionally, to the extent that Apple argues that it has no duty to review or evaluate apps and that it has disclaimed any liability arising from the actions of third parties, this argument both ignores contradictory statements made by Apple itself, and the allegations asserted by Plaintiffs regarding Apple's own conduct with respect to the alleged privacy violations. For one, it is not clear that Apple disclaimed all responsibility for privacy violations because, while Apple claimed not to have any liability or responsibility for any third party materials, websites or services, Apple also made affirmative representations that it takes precautions to protect consumer privacy. Additionally, Plaintiffs' allegations go beyond asserting that Apple had a duty to review or police third party apps. Instead, Plaintiffs allege Apple was responsible for providing user's information to third parties. AC ¶¶ 25, 30. Plaintiffs allege that Apple is independently liable for any statutory violations that have occurred. At the motion to dismiss stage, then, the Court is not prepared to rule that the Agreement establishes an absolute bar to Plaintiffs' claims.
…

III. CONCLUSION

For the reasons stated above, the Court DENIES Defendants' motions to dismiss pursuant to Rule 12(b)(1). However, the Court GRANTS the Mobile Industry Defendants' motion to dismiss pursuant to Rule 12(b)(6) in its entirety, without leave to amend. The Court GRANTS in part, and DENIES in part, Apple's motion to dismiss pursuant to Rule 12(b)(6). Specifically, Plaintiffs' claims against Apple for violations of the Stored Communications Act, violations of the Wiretap Act, violations of the California Constitutional right to privacy, negligence, violations of the Computer Fraud and Abuse Act, trespass, conversion, and unjust enrichment/assumpsit/ restitution are dismissed without leave to amend. The claims against Apple for violations of the UCL and CLRA survive the motion to dismiss.

IT IS SO ORDERED.
Footnotes
…
2. The Court refers to the "iDevice Class" and the "Geolocation Class" even though these classes have not been certified pursuant to Federal Rule of Civil Procedure 23. Any reference to "classes" within this Order is merely for ease of discussion and is not intended to imply a position regarding whether either class would be certifiable under the federal rules.
...
4. The Mobile Industry Defendants also argue that Plaintiffs lack prudential standing to bring an SCA claim. Mobile Industry MTD at 17. Because the Court finds, on other grounds, that Plaintiffs have failed to state a claim for relief under the SCA, the Court need not address this argument. *See Indep. Living Ctr. of S. Cal., Inc. v. Shewry*, 543 F.3d 1050, 1065 n. 17 (9th Cir.2008) ("Unlike the Article III standing inquiry, whether [Plaintiff] maintains prudential standing is not a jurisdictional limitation.") (citations omitted).

5. Apple also argues that it cannot be liable under the CFAA for negligent software design. *See* 18 U.S.C. § 1030(g) ("No cause of action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware."). However, this argument is unpersuasive at the pleading stage in light of the fact that Plaintiffs allege that Apple has been *intentionally* collecting Plaintiffs' geolocation data. *See* AC ¶¶ 115, 137.
...

LaCourt v. Specific Media, Inc.

United States District Court,
C.D. California.
April 28, 2011
Not Reported in F.Supp.2d
(Only the Westlaw citation is currently available)
2011 WL 1661532
No. SACV 10–1256–GW(JCGx).

Opinion

STATUS CONFERENCE

GEORGE H. WU, District Judge.
…

Tentative Ruling on Motion to Dismiss

I. Introduction

This case is one of a constellation of class action lawsuits pending before this Court which arise from the alleged use of Adobe Flash local shared objects ("LSOs" or "Flash Cookies") to track class members' use of the Internet without their knowledge or consent. Several consolidated cases related to this action—Valdez v. Quantcast Corporation, CV–10–5484–GW(JCGx); Aguirre v. Quantcast Corporation, CV 10–5716–GW(JCGx); White v. Clearspring Technologies, Inc., CV–10–5948–GW(JCGx); Intzekostas v. Fox Entertainment Group, CV–10–6586–GW(JCGx); and Davis v. VideoEgg, Inc., CV–10–7112–GW(JCGx)—have been resolved in a global settlement agreement which was preliminarily approved by this Court on March 30, 2011. In the present action, Defendant Specific Media, Inc. ("Specific Media") moves the Court for an Order dismissing the First Amended Consolidated Class Action Complaint pursuant to (inter alia) Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure.

II. Background

"Specific Media is an online third-party ad network that earns its revenue by delivering targeted advertisements." First Amended Consolidated Class Action Complaint ("FACC") ¶ 8. It uses HTTP cookies containing unique identifiers and browsing history information to track users in order to create behavioral profiles to target specific categories of ads at different users. See id. at ¶ 13. Allegedly, Specific Media used LSOs in order to circumvent the privacy and security controls of users who had set their browsers' to block third-party HTTP cookies, block Specific Media's HTTP cookies, or who deleted Specific Media's HTTP cookies. Id. at ¶ 17. In addition, it used LSOs to restore or "re-spawn" Specific Media HTTP cookies that were deleted by users. Id. at ¶ 18.

Plaintiff Genevieve LaCourt and the six other plaintiffs (hereinafter, "Plaintiffs") purport to represent a class consisting of "[a]ll persons residing in the United States who, during the Class

Period, used any web browsing program on any device to access web pages during which time and related to which Specific Media stored Adobe Flash local shared objects (LSOs) on such persons' computers." Id. at ¶ 35. Each of the named plaintiffs allege that they "are persons who have set the privacy and security controls on their browsers to block third-party cookies and/or who periodically delete third-party cookies," and that they each had a "Flash cookie" installed on their computer by Specific Media without their notice or consent. Id. at ¶¶ 21, 24.

*2 Plaintiffs allege that they sought to maintain the secrecy and confidentiality of the information obtained by Defendant through the use of LSOs. Id. at ¶ 30. They further allege that "Defendant's conduct has caused economic loss to Plaintiffs and Class Members in that their personal information has discernable value, both to Defendant and to Plaintiffs and Class Members, and of which Defendant has deprived Plaintiffs and Class Members and, in addition, retained and used for its own economic benefit." Id. at ¶ 38.

Based on the above allegations, Plaintiffs have asserted the following claims for relief on behalf of themselves and the class: (1) Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Violation of Computer Crime Law, Cal.Penal Code § 502; (3) Violations of Invasion of Privacy Act, Cal.Penal Code § 630; (4) Violation of Consumer Legal Remedies Act, Cal. Civ.Code § 1750; (5) Unfair Competition, Cal. Bus. and Prof.Code § 17200; (6) Trespass to Personal Property/Chattel; and (7) Unjust Enrichment.
…

IV. Analysis

A. Article III Standing

Defendant first argues that the Court lacks subject matter jurisdiction over this action because Plaintiffs have failed to allege "the irreducible constitutional minimum of standing" required by Article III of the Constitution, i.e., the existence of an actual case or controversy. Krottner v. Starbucks Corp., 628 F.3d 1139, 1141 (9th Cir.2010) (quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)). In order to establish standing, a plaintiff must show: "(1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." Id. (quoting Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000)). Here, Specific Media challenges only Plaintiffs' ability to satisfy the first of these requirements, asserting that Plaintiffs have failed to plausibly allege an "injury in fact."

1. Plaintiffs have not alleged that any named Plaintiff was affected by Defendant's alleged conduct.

Specific Media argues that Plaintiffs, upon close reading of the Complaint, have not alleged that Specific Media ever actually tracked the online activity of any named plaintiff, or that Plaintiffs ever deleted any Specific Media browser cookies, or that Plaintiffs' browser cookies were ever "re-spawned" by Specific Media. Rather, the Complaint simply alleges that Specific Media

installed Flash cookies on Plaintiffs' computers and then states that “Plaintiffs believe that, if they were to re-visit the websites on which Specific Media [Flash cookies] were set, or were to visit other websites on which Specific Media served online advertisements, the tracking devices would be used as substitutes for HTTP cookies and to re-spawn previously deleted cookies.” FACC ¶ 25. Thus, Specific Media argues, to the extent that Plaintiffs have alleged any injury at all, it is one that is entirely conjectural, hypothetical, or speculative.

*4 Plaintiffs' mere use of the subjunctive does not mean that they have not alleged an injury that is “imminent.” The threat that Plaintiffs' previously deleted cookies will be re-spawned when they visit websites in the Specific Media's network is, potentially, a threat of imminent harm sufficient to satisfy the “injury in fact” requirement of standing. However, it is not clear that Plaintiffs have even alleged this. Plaintiffs assert, in a footnote to their opposition, that they have “indeed allege[d] that Specific Media installed LSOs to track [Plaintiffs'] online activities and that they deleted Specific Media browser cookies.” Opp. 4 n.3. Except for the conclusory allegation at ¶ 1 (“Nature of the Case”), however, the portions of the FACC they cite, namely ¶¶ 13–19, describing the nature of Specific Media's alleged practices, do not specifically allege that Plaintiffs themselves were affected by them. An inference might be drawn, but rather than invite an argument over the reasonableness of such an inference, Plaintiffs should have specifically alleged that they were affected by Defendant's alleged practices.

2. Plaintiffs have not alleged an economic injury or harm to their computers.

Even assuming Plaintiffs can allege that they were affected by Specific Media's alleged practices regarding Flash Cookies, an even more difficult question is whether they can allege that they were injured by them. In this respect, Plaintiffs' Opposition is surprisingly tepid. In addition to simply repeating the conclusory statements in their Complaint to the effect that Defendant's conduct has caused them to suffer an injury, Plaintiffs refer to a host of facts—including facts pertaining to the value of their personal information and to the supposedly deleterious effects that Defendant's LSOs had on Plaintiffs' computers—that are not contained in their Complaint at all.

The parties in their papers engage in a quasi-philosophical debate about the possible value of consumers' “personal information” on the Internet. Ultimately, the Court probably would decline to say that it is categorically impossible for Plaintiffs to allege some property interest that was compromised by Defendant's alleged practices.[1] The problem is, at this point they have not done so. Plaintiffs—who have more or less completely accepted Defendant's framing of the issue—make the problematic argument that “by taking and retaining [Plaintiffs'] personal information,” i.e., their browsing history, Defendant has deprived Plaintiffs of this information's economic value. The theory underlying this assertion is presented by reference to a number of academic articles concerning the nature of “Internet business models ... driven by consumers' willingness to supply data about themselves.” Opp. 5:6–7. While the Court would recognize the viability in the abstract of such concepts as “opportunity costs,” “value-for-value exchanges,” “consumer choice,” and other concepts referred to in the Opposition, what Plaintiffs really need to do is to give some particularized example of their application in this case.

*5 Defendant aptly notes that the Complaint does not identify a single individual who was foreclosed from entering into a “value-for-value exchange” as a result of Specific Media's

alleged conduct. Furthermore, there are no facts in the FACC that indicate that the Plaintiffs themselves ascribed an economic value to their unspecified personal information. Finally, even assuming an opportunity to engage in a "value-for-value exchange," Plaintiffs do not explain how they were "deprived" of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party.

In addition to the injury based on the supposed loss of their personal information. Plaintiffs also half-heartedly argue that they suffered harm to their computers "because Specific Media's installation of Flash LSOs circumvented and diminished the performance and capabilities of their computers." Opp. 9:18–20. If the loss of the ability to delete cookies counts[2] as harm to Plaintiffs' computers, then maybe Plaintiffs have alleged some de minimis injury, but probably not one that would give rise to Article III standing. If Plaintiffs are suggesting that their computers' performance was compromised in some other way—a claim that was made in the first iteration of the Complaint but all but abandoned in the FACC—then they need to allege facts showing that this is true.

3. In re Doubleclick

At least one case, In re DoubleClick Privacy Litigation, 154 F.Supp.2d 497 (S.D.N.Y.2001), has held—albeit not in the context of evaluating Article III standing—that website visitors do not suffer a cognizable "economic loss" from the collection of their data. In Doubleclick, the court rejected plaintiffs' arguments that they suffered economic damages for the purpose of stating a claim under the Computer Fraud and Abuse Act based on both (1) the economic value of their attention to Doubleclick's advertisements (which is not an argument that Plaintiffs in this case make) and (2) the value of the demographic information compiled by it through the use of browser cookies (which basically is). Id. at 524. In particular, the court wrote that "although demographic information is valued highly ... the value of its collection has never been considered a economic loss to the subject." Id. at 525. While Plaintiffs attempt to distinguish DoubleClick on the ground they have alleged that they were deprived not of "mere demographic information," but "of the value of their personal data," it is not clear what they mean by this. Defendant observes that, if anything, the Plaintiffs in Doubleclick alleged that the defendant collected much more information than Specific Media supposedly collected in this case, including "names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect." Id. at 503.

*6 Doubleclick, obviously, is not binding on this Court. Its reasoning at least suggests that the question of Plaintiffs' ability to allege standing is a serious one, however. It would be very difficult to conclude at this point that Plaintiffs have met their burden of establishing that this Court has subject matter jurisdiction. Specific Media goes too far, though, when in the introductory section of its opening brief it accuses Plaintiffs (and their lawyers) of bringing this action in bad faith.[3] Specific Media maintains that the practices of using LSOs to re-spawn browser cookies or to surreptitiously track computer users' visits to websites are utterly innocuous at the same time it denies engaging in them. All of the defendants in the related actions have disavowed such practices and have promised to take steps to prevent them. It is not obvious that Plaintiffs cannot articulate some actual or imminent injury in fact. It is just that at

this point they haven't offered a coherent and factually supported theory of what that injury might be.

B. Specific Causes of Action

In light of Plaintiffs' apparent inability to allege a basis for standing, a lengthy discussion of the defects (many of which are related to the standing issue) of the specific causes of action alleged in the FACC would be an inefficient use of time. Some points would nevertheless be noted.

1. The CFAA

First, with respect to the CFAA, it is doubtful that Plaintiffs have the ability to state a claim under this statute. The CFAA permits a person that "suffers damage or loss" by reason of a violation of the CFAA, to "maintain a civil action against the violator" for damages and injunctive relief. 18 U.S.C. § 1030(g). The CFAA defines "damage" as "any impairment to the integrity or availability of data, a system, or information." 18 U.S.C. § 1030(e)(8) (emphasis added). The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Plaintiffs must claim economic loss or damages in an amount "aggregating at least $5,000 in value during any 1–year period to one or more individuals." 18 U.S.C. § 1030(c)(4)(A)(i)(I).[4] Defendant correctly observe that based on the above discussion regarding standing, Plaintiffs at the very least have failed to plausibly allege that they and the putative class—even in the aggregate—have suffered $5,000 in economic damages in a one year period as a result of Specific Media's actions.

There may well be other problems with this claim. For example, Plaintiffs contend that Specific Media violated Section (a)(5)(A) of the CFAA, but it is unclear whether Specific Media can be said to have "intentionally caus[ed] damage" to Plaintiffs' computers. 18 U.S.C. § 1030(a)(5)(A). These questions, however, are rather less likely to be able to be resolved at the pleading stage.
…

4. Trespass to Chattels

The tort of trespass to chattels has been extended to cases where the plaintiff can establish that "(1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in [a] computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff." eBay, Inc. v. Bidder's Edge, Inc., 100 F.Supp.2d 1058, 1069–1070 (N.D.Cal.2000). The California Supreme Court has held that the tort "does not encompass ... an electronic communication that neither damages the recipient computer system nor impairs its functioning." Intel Corp. v. Hamidi, 30 Cal.4th 1342, 1347 (2003); see also id. at 1356 ("In the decisions so far reviewed, the defendant's use of the plaintiff's computer system was held sufficient to support an action for trespass when it actually did, or threatened to, interfere with the intended functioning of the system, as by significantly reducing its available memory and processing power."). Here, Plaintiffs have not alleged that the functioning of their computers was

impaired (except in the trivial sene of being unable to permanently delete cookies) or would be imminently impaired to the degree that would enable them to plead the elements of the tort. Moreover, ebay, Inc., in which the defendant did not dispute that it had employed an automated computer program to search eBay's electronic database and continued to do so even after eBay demand that it stop, 100 F.Supp.2d at 1070, is readily distinguishable from this case on the question of authorization.

5. UCL and CLRA claims

*8 Plaintiffs in their Opposition do not attempt to defend the legal viability of their CLRA claim, and Defendant appears to be correct that they cannot state such a claim. The UCL claim also is problematic, if for no other reason than Plaintiffs' apparent lack of standing. It is not completely clear, however, that Plaintiffs ultimately would not be able to state a viable claim under the "unfairness" prong of the UCL. If Plaintiffs intend to attempt to state a claim under the "fraud" prong of the statute, they should be advised that Rule 9(b) would apply to such a claim.

6. Unjust Enrichment

This Court agrees with other courts in this district that "unjust enrichment is not an independent claim," and hence cannot serve as an independent cause of action. In re DirecTV Early Cancellation Litig., 738 F.Supp.2d 1062, 1091 (C.D.Cal.2010).

V. Conclusion

For the above reasons, Defendant's Motion to Dismiss would be GRANTED WITH LEAVE TO AMEND.

Footnotes

1. Or, for that matter, some type of privacy interest. It is noted that at ¶ 26 of the FACC Plaintiffs allege that "Plaintiffs consider information about their online activities to be in the nature of confidential information that they protect from disclosure, including by periodically deleting cookies."
2. There is a question as to whether that loss was temporary or permanent.
3. Defendant's counsel would be instructed that lawyers should not, just as a matter of basic professionalism, accuse other lawyers of operating a "shakedown" operation unless they can completely support such accustions.
4. Although Defendant does not dispute this point, it would appear somewhat questionable as to whether Plaintiffs may permissibly aggregate the claims of the entire class to reach the $5,000 limit. Section 1030(c)(4)(A)(i)(I) speaks of "loss to 1 or more persons during any 1–year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $ 5,000 in value." It is not clear that, in a civil action not brought by the United States, harm to different persons over a one-year period can be aggregated unless it relates to conduct affecting a single computer.

Facebook, Inc. v. Power Ventures, Inc.

United States District Court,
N.D. California, San Francisco Division.
February 16, 2012
844 F.Supp.2d 1025

Opinion

ORDER GRANTING PLAINTIFF'S MOTIONS FOR SUMMARY JUDGMENT; DENYING DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

JAMES WARE, Chief Judge.

I. INTRODUCTION

Facebook, Inc. ("Plaintiff") brings this action against Defendants alleging violations of the Controlling the Assault of Non–Solicited Pornography and Marketing Act ("CAN–SPAM Act"), 15 U.S.C. §§ 7701 et seq., the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and California Penal Code § 502. Plaintiff alleges that Defendants accessed its website in an unauthorized manner, and then utilized this unauthorized access to send unsolicited and misleading commercial e-mails to Facebook users.

Presently before the Court are Plaintiff's Motions for Summary Judgment on Counts One, Two and Three, and Defendants' Motion for Summary Judgment on all counts. The Court conducted a hearing on January 23, 2012. Based on the papers submitted to date and oral argument, the Court GRANTS Plaintiff's Motions for Summary Judgment on all counts, and DENIES Defendants' Motion for Summary Judgment.

II. BACKGROUND

A. Undisputed Facts

Plaintiff owns and operates the widely popular social networking website located at http://www.facebook.com. Defendant Power is a corporation incorporated in the Cayman Islands doing business in the State of California. Defendants operate a website, www.power.com, which offers to integrate multiple social networking accounts *1028 into a single experience on Power.com. (FAC ¶ 5; Answer ¶ 5.) Defendant Vachani is the CEO of Power. (Id. ¶ 11; Id. ¶ 11.)

Users of Plaintiff's website register with a unique username and password. (FAC ¶ 21; Answer ¶ 21.) Before Plaintiff activates a username and permits a user to access certain features of Facebook, the user must agree to Plaintiff's Terms of Use. (Id. ¶ 29; Id. ¶ 29.) The Terms of Use require users to refrain from using automated scripts to collect information from or otherwise

interact with Facebook, impersonating any person or entity, or using Facebook website for commercial use without the express permission of Facebook. (Id. ¶ 30; Id. ¶ 30.)

On or before December 1, 2008, Power began advertising and offering integration with Plaintiff's site. (FAC ¶ 49; Answer ¶ 49.) Power permitted users to enter their Facebook account information and access Facebook site through Power.com. (Id. ¶ 50; Id. ¶ 50.) At no time did Defendants receive permission from Plaintiff to represent that solicitation of Facebook usernames and passwords was authorized or endorsed by Plaintiff. (Id. ¶ 53; Id. ¶ 53.)

On or before December 26, 2008, Power began a "Launch Promotion" that promised Power.com's users the chance to win one hundred dollars if they successfully invited and signed up new Power.com users. (FAC ¶ 65; Answer ¶ 65.) As part of this promotion, Power provided participants with a list of their Facebook friends, obtained by Power from Facebook, and asked the participant to select which of those friends should receive a Power invitation. (Id. ¶ 66; Id. ¶ 66.) The invitations sent to those friends purport to come from "Facebook" and used an "@facebookmail.com" address, not a Power.com address. (Id. ¶ 68; Id. ¶ 68.)

On December 1, 2008, Plaintiff notified Defendant Vachani of its belief that Power's access of Plaintiff's website and servers was unauthorized and violated Plaintiff's rights. (FAC ¶ 57; Answer ¶ 57.) Facebook subsequently implemented technical measures to block users from accessing Facebook through Power.com. (Id. ¶ 63; Id. ¶ 63.)
…

IV. DISCUSSION

Plaintiff moves for summary judgment on the grounds that: (1) the undisputed evidence establishes that Defendants sent misleading commercial e-mails through Facebook's network in violation of the CAN–SPAM Act;[8] and (2) the undisputed *1030 evidence also establishes that Defendants utilized technical measures to access Facebook without authorization, in violation of both the CFAA and California Penal Code Section 502. Defendants respond that: (1) because Plaintiff's own servers sent the commercial e-mails at issue, Defendants did not initiate the e-mails as a matter of law; and (2) Defendants did not circumvent any technical barriers in order to access Facebook site, precluding liability under the CFAA or Section 502. Defendants further contend that Plaintiff suffered no damages as a result of Defendants' actions, and thus lacks standing to bring a private suit for Defendants' conduct. (Id. at 15–16, 19–20.)

A. The CAN–SPAM Act

At issue is whether the conduct of Defendants, as established by the undisputed evidence, constitutes a violation of the CAN–SPAM Act.

The CAN–SPAM Act provides that "[i]t is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). The Act also creates a private right of action for internet service providers adversely affected by violations of this provision. See id. §

7706(g)(1). To prevail on a CAN–SPAM Act claim, a plaintiff must establish not only that the defendant violated the substantive provisions of the Act, but also that the plaintiff was adversely affected by this violation such that it satisfies the statutory standing requirements. See Gordon v. Virtumundo, Inc., 575 F.3d 1040, 1048 (9th Cir.2009). The Court considers each requirement in turn.

1. Standing

At issue is whether Plaintiff has standing to assert a claim under the CAN–SPAM Act.

Standing under Section 7706 "involves two general components: (1) whether the plaintiff is an 'Internet access service' provider ('IAS provider'), and (2) whether the plaintiff was 'adversely affected by' statutory violations." Gordon, 575 F.3d at 1049 (citation omitted).

Here, Defendants concede that Plaintiff is an IAS provider. Therefore, the only question before the Court in determining Plaintiff's standing is whether Plaintiff was "adversely affected" by the alleged violations at issue.

In Gordon, the Ninth Circuit explained that not all possible harms to an IAS provider constitute harm within the meaning of the Act, and distinguished those harms sufficient to confer standing from those outside the scope of Congress' intent. See 575 F.3d at 1049–55. After discussing the congressional decision to confer standing upon IAS providers but not end-consumers affected by commercial e-mails, the court concluded that "[l]ogically, the harms redressable under the CANSPAM Act must parallel the limited private right of action and therefore should reflect those types of harms uniquely encountered by IAS providers." Id. at 1053. Thus, while the "mere annoyance" of spam encountered by all e-mail users is not sufficient to confer standing, the court identified the costs of investing in new equipment to increase capacity, customer service personnel to address increased *1031 subscriber complaints, increased bandwidth, network crashes, and the maintenance of anti-spam and filtering technologies as the "sorts of ISP-type harms" that Congress intended to confer standing. Id. at 1053. Thus, the court noted, "[i]n most cases, evidence of some combination of operational or technical impairments and related financial costs attributable to unwanted commercial e-mail would suffice." Id. at 1054 (citation omitted).

Here, in support of its contention that it has standing to pursue a CANSPAM Act claim, Plaintiff offers the following evidence:

(1) Around December 1, 2008 Ryan McGeehan, manager of Plaintiff's Security Incident Response Team ("SIR Team"), determined that Power was running an automated scripting routine to harvest data and download it to the Power.com website. McGeehan then spent substantial time and effort determining what steps were necessary to contain Power's spamming. (Id. ¶ 12.) It was determined that at least 60,627 event invitations were sent to Facebook users due to Power's activities. (Id.) On December 12, 2008, after Plaintiff's counsel sent Power a cease and desist letter, and the activity did not stop, Plaintiff attempted to block Power's access by blocking what appeared to be its primary IP address. (Id. ¶ 13.) On December 22, 2008, McGeehan determined that Power was still accessing Facebook through new IP addresses. (Id. ¶

14.) Plaintiff then attempted to block these IP addresses as well. (Id. ¶ 13.) In early 2009, Facebook blacklisted the term Power.com, preventing that term from appearing anywhere on the site. (Id. ¶ 16.) In implementing these measures, McGeehan spent at least three to four days of his own engineering time addressing security issues presented by Power. (Id. ¶ 17.)

(2) On December 1, 2008, Joseph Cutler sent a cease and desist letter to Power.com. After this letter was sent Cutler was contacted by Steve Vachani, who identified himself as the owner and operator of Power Ventures. (Id. ¶ 7.) In this and subsequent discussions, Vachani assured Cutler that the functionality of the Power website would be changed to comply with Facebook's requests. (Id. ¶¶ 9–10.) On December 27, 2008, Cutler received an e-mail saying that Power Ventures would not change its website as earlier stated. (Id. ¶ 13.) From fall of 2008 through early 2009, Facebook spent approximately $75,000 on Cutler's firm related to Power Venture's actions. (Id. ¶ 15.)

Defendants do not dispute the accuracy or veracity of this evidence of Plaintiff's expenditures. Instead, Defendants contend that, as a matter of law, these are not the sorts of harm that give rise to standing under Gordon, as they fall within the category of negligible burdens routinely borne by IAS providers. In support of this *1032 contention, Defendants rely on the following evidence:

(1) In the fourth quarter of 2008, Plaintiff received 71,256 user complaints that contained the word “spam.” (McGeehan Decl. ¶ 5.) Facebook did not produce any evidence of customer complaints specifically referencing the e-mails at issue in this case.

(2) Craig Clark, litigation counsel at Facebook, testified that he was not aware of any documents that would be responsive to any of the requests for production made by Defendants.[17] These requests for production included requests for all documents regarding any injury that Plaintiff suffered, expenditures Plaintiff made, or user complaints that Plaintiff received as a result of the events complained of in Plaintiff's First Amended Complaint.

Upon review, on the basis of these undisputed facts, the Court finds that Plaintiff has demonstrated an “adverse effect” from Defendants' conduct sufficient to confer standing. The evidence submitted by Plaintiff is not limited to documenting a general response to spam prevention, but rather shows acts taken and expenditures made in response to Defendants' specific acts. These specific responses to Defendants' actions distinguish Plaintiff's damages from those in the cases relied upon by Defendants, which asserted only the costs of general spam prevention as the basis for standing.[20] In particular, since Plaintiff documented a minimum of 60,000 instances of spamming by Defendants, the costs of responding to such a volume of spamming cannot be categorized as “negligible.” See Gordon, 575 F.3d at 1055–56. The Court finds that under Gordon and Azoogle, though the general costs of spam prevention may not confer standing under the CAN–SPAM Act, documented expenditures related to blocking a specific offender may. This is particularly true where, as here, Defendants' spamming activity was ongoing, prolific, and did not stop after requests from the network owner. Thus, as the undisputed evidence establishes that Plaintiff expended significant resources to block Defendants' specific spamming activity, the Court finds that Plaintiff has standing to maintain a CANSPAM action.

2. Merits of CAN–SPAM Act Claim

At issue is whether Defendants' conduct, as established by the undisputed facts, violates the substantive provisions of the *1033 CAN–SPAM Act. The Act makes it unlawful, inter alia, "for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading." 15 U.S.C. § 7704(a)(1). Defendants contend that Plaintiff's CAN–SPAM Act claim must fail because: (1) the undisputed facts establish that Plaintiff itself, and not Defendants, initiated the e-mails at issue; and (2) because Plaintiff sent the e-mails, the header information identifying Facebook as the sender was accurate and not misleading. The Court considers each element in turn.

a. Initiation of Commercial E-mails

At issue is whether Defendants initiated the e-mails associated with the Launch Promotion.

The CAN–SPAM Act provides that "[t]he term 'initiate,' when used with respect to a commercial electronic mail message, means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of such message. For purposes of this paragraph, more than one person may be considered to have initiated a message." 15 U.S.C. § 7702(9). The word "procure," in turn, is defined to mean "intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one's behalf." Id. § 7702(12).
…

Upon review, the Court finds that based on these undisputed facts, Defendants initiated the e-mails sent through the Launch Promotion. Although Facebook servers did automatically send the e-mails at the instruction of the Launch Program, it is clear that Defendants' actions-in creating the Launch Promotion, importing users' friends to the guest list, and authoring the e-mail text-served to "originate" the e-mails as is required by the Act.[26] To hold that Plaintiff originated the e-mails merely because Facebook servers sent them would ignore the fact that Defendants intentionally caused Facebook's servers to do so, and created a software program specifically designed to achieve that effect. Further, while Defendants emphasize that Facebook users authorized the creation of events resulting in the e-mails, the Court finds that Defendants procured these users to do so by offering and awarding monetary incentives to provide such authorization. Thus, even if Facebook users may be viewed as initiators of the e-mails because of their participation in the Launch Promotion, Defendants are nonetheless also initiators as a matter of law because of their procurement of user participation.[28]

Accordingly, the Court finds that Defendants did initiate the e-mails at issue within the meaning of the CAN–SPAM Act.

b. Whether the E-mails Are Misleading

At issue is whether the e-mails sent as a result of the Launch Promotion contain header information that is false or misleading.

The CAN–SPAM Act defines header information as "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." 15 U.S.C. § 7702(8). The Act further provides that "header information shall be considered materially misleading if it fails to identify accurately a protected computer used to initiate the message because the person *1035 initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin." Id. § 7704(a)(1)(C). A false or misleading statement is considered material if "the alteration or concealment of header information" would impair the ability of an IAS provider or a recipient to "identify, locate, or respond to a person who initiated the electronic mail message." Id. § 7704(a)(6).

Here, for the reasons discussed above, Defendants were initiators of the e-mail messages at issue. But because Defendants' program caused Facebook servers to automatically send the e-mails, these e-mails contained an "@facebookmail.com" address. These e-mails did not contain any return address, or any address anywhere in the e-mail, that would allow a recipient to respond to Defendants. Thus, as the header information does not accurately identify the party that actually initiated the e-mail within the meaning of the Act, the Court finds that the header information is materially misleading as to who initiated the e-mail.
…

In sum, the Court finds that the undisputed facts establish that Defendants initiated *1036 the sending of e-mails with false or misleading heading information under the CAN–SPAM Act, and that Plaintiff suffered adverse effects as contemplated by the Act sufficient to convey standing to maintain a private cause of action. Accordingly, the Court GRANTS Plaintiff's Motion for Summary Judgment on Count One, and DENIES Defendants' Motion for Summary Judgment as to Count One.

…
C. The Computer Fraud and Abuse Act

At issue is whether Defendants' conduct constitutes a violation of the CFAA.

The CFAA imposes liability on any party that "intentionally accesses a computer *1039 without authorization or exceeds authorized access, and thereby obtains," inter alia, "information from any protected computer." 18 U.S.C. § 1030(a)(2). Suit may be brought by any person who suffers damage or loss in an amount above $5000. See Id. § 1030(g); § 1030(c)(4)(A)(i)(I).

Here, for the reasons discussed above, the undisputed facts establish that Defendants' access to Facebook was without authorization. In addition, Defendants admit that they obtained information from Facebook website. (Defendants' Admissions at 22.) Thus, the only finding necessary for Plaintiff to prevail on its CFAA claim is whether Plaintiff's damages exceed $5000, thereby giving Plaintiff standing under the statute.[43]

The CFAA defines “loss” to include “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.” 18 U.S.C. § 1030(e)(11). “Costs associated with investigating intrusions into a computer network and taking subsequent remedial measures are losses within the meaning of the statute.” Multiven, 725 F.Supp.2d at 895 (citation omitted).

7 Here, as discussed above with regard to Plaintiff's CAN–SPAM claim, Plaintiff has provided uncontradicted evidence of the costs of attempting to thwart Defendants' unauthorized access into its network. These documented costs were well in excess of the $5000 CFAA threshold. (See Cutler Decl. ¶ 15.) Thus, the Court finds that on the basis of these costs, Defendants' unauthorized access of Plaintiff's network did cause sufficient loss to Plaintiff to confer standing upon Plaintiff.

In sum, for the reasons discussed above regarding Plaintiff's Section 502 claim, the Court finds that Defendants accessed Plaintiff's website without authorization and obtained information from Facebook. The Court further finds that Plaintiff suffered loss sufficient to confer standing as a result of such access. Accordingly, the Court GRANTS Plaintiff's Motion for Summary Judgment as to Count Two and DENIES Defendants' Motion for Summary Judgment as to Count Two.

V. CONCLUSION

The Court GRANTS Plaintiff's Motions for Summary Judgment on all counts. The Court DENIES Defendants' Motion for Summary Judgment on all counts.[45]
…

Footnotes

…
8. (CAN–SPAM MSJ at 12–16.)
…
17. (Fisher Decl., Ex. C, Deposition of Craig Clark at 118:20–118:23, hereafter, “Clark Depo.,” Docket Item No. 106.) Plaintiff objects to Defendants' reliance on Mr. Clark's testimony because Mr. Clark was deposed in his personal capacity, rather than pursuant to Fed.R.Civ.P. 30(b)(6), and thus Plaintiff contends that Mr. Clark's answers to the questions presented to him are irrelevant because he does not speak on behalf of Facebook. (See Docket Item No. 240 at 17–23.) For the purposes of this Order only, Plaintiff's objection to the Clark deposition is OVERRULED because harm to Plaintiff is established irregardless of Mr. Clark's testimony.
…
20. (See, e.g., CAN–SPAM Opp'n at 15) (citing ASIS Internet Servs. v. Azoogle.com, Inc., 357 Fed.Appx. 112, 113–14 (9th Cir.2009)).
…
26. See 15 U.S.C. § 7702(9).
…

28. See 15 U.S.C. § 7702(12).

…

43. See Multiven, Inc. v. Cisco Sys., Inc., 725 F.Supp.2d 887, 895 (N.D.Cal.2010) (explaining that elements of a CFAA claim do not differ materially from the elements of a claim under Section 502).

…

45. Because the Court finds that the undisputed evidence submitted by Plaintiff with its Motions for Summary Judgment establishes that Plaintiff is entitled to judgment as a matter of law, the Court DENIES as moot Plaintiff's Motion to File Supplemental Evidence. (See Docket Item No. 251.)

In addition, the Court DENIES as moot Plaintiff's Motion to Enlarge Time for Hearing Dispositive Motions. (See Docket Item No. 261.)

In re Zappos.com, Inc., Customer Data Sec. Breach Litigation

United States District Court,
D. Nevada.
September 27, 2012
893 F.Supp.2d 1058

Opinion

Order

ROBERT C. JONES, Chief Judge.

This Multidistrict Litigation ("MDL") proceeding arises out of a security breach of servers belong to Defendants Amazon.com, Inc. ("Amazon"),[1] doing business *1061 as Zappos.com, and Zappos.com, Inc. ("Zappos") in January 2012. Now pending is Defendant Zappos' Motion to Compel Arbitration and Stay action (# 3).

I. Relevant Factual Background

Zappos is an online retailer of apparel, shoes, handbags, home furnishing, beauty products, and accessories. (Rajan Decl. ¶ 3 (# 3–1).) Plaintiffs are Zappos customers who gave personal information to Zappos in order to purchase goods via Zappos.com and/or 6PM.com. (Id. ¶¶ 4–7; Rajan Second Supp'l Decl. ¶¶ 3–13 (# 13–1).) In mid-January 2012, a computer hacker attacked Zappos.com and attempted to download files containing customer information such as names and addresses from a Zappos server (the "Security Breach"). (Defs.' Mot. Compel at 1(# 3); Pls.' Opp'n at 4(# 10).) Plaintiffs allege that on January 16, 2012, Zappos notified Plaintiffs via email that their personal customer account information had been compromised by hackers. (Def.'s Mot. Compel at 6 (# 3); Steven Pls.' Opp'n at 1(# 9); Pls.' Opp'n at 4(# 10).) Plaintiffs have filed complaints in federal district courts across the country seeking relief pursuant to state and federal statutory and common law for damages resulting from the Security Breach.

…

*1062 III. Legal Standard

The Federal Arbitration Act ("FAA") provides that contractual arbitration agreements "shall be valid, irrevocable, and enforceable, save upon such grounds as exist at law or in equity for the revocation of any contract." 9 U.S.C. § 2. Arbitration agreements are enforced under sections 3 and 4 of the FAA, which provide "two parallel devices for enforcing an arbitration agreement." Moses H. Cone Mem'l Hosp. v. Mercury Constr. Corp., 460 U.S. 1, 22, 103 S.Ct. 927, 74 L.Ed.2d 765 (1983). Section 3 gives courts the power to provides "a stay of litigation in any case raising a dispute referable to arbitration," while section 4 empowers courts to provide "an affirmative order to engage in arbitration." Id.; 9 U.S.C. §§ 3–4.

The FAA "is a congressional declaration of a liberal federal policy favoring arbitration agreements, notwithstanding any state substantive or procedural policies to the contrary." Moses H. Cone Mem'l Hosp., 460 U.S. at 24, 103 S.Ct. 927; see also Southland Corp. v. Keating, 465 U.S. 1, 2, 104 S.Ct. 852, 79 L.Ed.2d 1 (1984) (finding that the FAA "declared a national policy favoring arbitration"); Perry v. Thomas, 482 U.S. 483, 489, 107 S.Ct. 2520, 96 L.Ed.2d 426 (1987) (stating that the FAA "embodies a clear federal policy requiring arbitration" when there is a written arbitration agreement relating to interstate commerce). Thus, "an order to arbitrate [a] particular grievance should not be denied unless it may be said with positive assurance that the arbitration clause is not susceptible of an interpretation that covers the asserted dispute." United Steelworkers of Am. v. Warrior & Gulf Navigation Co., 363 U.S. 574, 582–83, 80 S.Ct. 1347, 4 L.Ed.2d 1409 (1960).

Despite this strong federal policy in favor of arbitration, arbitration is a "matter of contract," and no party may be required to submit to arbitration "any dispute which he has not agreed so to submit." Howsam v. Dean Witter Reynolds, Inc., 537 U.S. 79, 79, 123 S.Ct. 588, 154 L.Ed.2d 491 (2002) (quoting United Steelworkers, 363 U.S. at 582, 80 S.Ct. 1347); see also Volt Info. Scis., Inc. v. Bd. of Trs. of Leland Stanford Junior Univ., 489 U.S. 468, 478, 109 S.Ct. 1248, 103 L.Ed.2d 488 (1989) ("[T]he FAA does not require parties to arbitrate when they have not agreed to do so."). A court's discretion for compelling arbitration is thus limited to a two-step process of "determining (1) whether a valid agreement to arbitrate exists, and if it does; (2) whether the agreement encompasses the dispute at issue." Chiron Corp. v. Ortho Diagnostic Sys., Inc., 207 F.3d 1126, 1130 (9th Cir.2000). A party cannot be ordered to arbitration unless there is "an express, unequivocal agreement to that effect." Samson v. NAMA Holdings, LLC, 637 F.3d 915, 923 (9th Cir. 2011) (quoting Par–Knit Mills, Inc. v. Stockbridge Fabrics Co., Ltd., 636 F.2d 51, 54 (3d Cir.1980)).

With regard to the determination of whether there is a valid agreement to arbitrate between the parties, "the liberal federal policy regarding the scope of arbitrable issues is inapposite." Comer v. Micor, Inc., 436 F.3d 1098, 1104 n. 11 (9th Cir.2006). Instead, federal courts "should apply ordinary state-law principles that govern the formation of contracts." First Options of Chicago, Inc. v. Kaplan, 514 U.S. 938, 944, 115 S.Ct. 1920, 131 L.Ed.2d 985 (1995). Under Nevada law,[5] "[b]asic contract principles require, for an enforceable contract, an offer and acceptance, *1063 meeting of the minds, and consideration." May v. Anderson, 121 Nev. 668, 119 P.3d 1254, 1257 (2005) (citing Keddie v. Beneficial Ins., Inc. 94 Nev. 418, 580 P.2d 955, 956 (1978) (Baltjer, C.J., concurring)). Put differently, an enforceable contract "requires a manifestation of mutual assent in the form of an offer by one party and acceptance thereof by the other ... [and] agreement or meeting of the minds of the parties as to all essential elements." (Keddie, 580 P.2d at 957 (citations omitted)).

IV. Discussion

The arbitration agreement at issue, founds in the Disputes section of the Terms of Use of the Zappos.com website, provides as follows:

> Any dispute relating in any way to your visit to the Site or to the products you purchase through the Site shall be submitted to confidential arbitration in Las Vegas, Nevada,

> except that to the extent you have in any manner violated or threatened to violate our intellectual property rights, we may seek injunctive or other appropriate relief in any state or federal court in the State of Nevada. You hereby consent to, and waive all defense of lack of personal jurisdiction and forum non conveniens with respect to venue and jurisdiction in the state and federal courts of Nevada. Arbitration under these Terms of Use shall be conducted pursuant to the Commercial Arbitration Rules then prevailing at the American Arbitration Association. The arbitrator's award shall be final and binding and may be entered as a judgment in any court of competent jurisdiction. To the fullest extent permitted by applicable law, no arbitration under this Agreement shall be joined to an arbitration involving any other party subject to this Agreement, whether through class action proceedings or otherwise. You agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of, related to or connected with the use of the Site or this Agreement must be filed within one (1) year after such claim or cause of action arose or be forever banned.

(Carton Decl. Ex. 8 (# 10–16).) Additionally, the first paragraph of the Terms of Use provides in relevant part: "We reserve the right to change this Site and these terms and conditions at any time. ACCESSING, BROWSING OR OTHERWISE USING THE SITE INDICATES YOUR AGREEMENT TO ALL THE TERMS AND CONDITIONS IN THIS AGREEMENT, SO PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PROCEEDING." (Id. (emphasis in original).)

A. Plaintiffs Did Not Agree to the Terms of Use

The Court's first step when presented with a motion to compel arbitration is to determine whether a valid agreement to arbitrate exists. Chiron Corp., 207 F.3d at 1130.

It is undisputed that Zappos' Terms of Use constitutes what federal courts have deigned a "browsewrap" agreement. With a browsewrap agreement, a website owner seeks to bind website users to terms and conditions by posting the terms somewhere on the website, usually accessible through a hyperlink located somewhere on the website; in contrast, a "clickwrap" agreement requires users to expressly manifest assent to the terms by, for example, clicking an "I accept" button. Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 22 n. 4 (2d Cir.2002) (J. Sotomayor). "Because no affirmative action is required by the website user to agree to the terms of a contract other than his or her use of the website, the determination of the validity of a browsewrap contract depends on whether the *1064 user has actual or constructive knowledge of a website's terms and conditions." Van Tassell v. United Mktg. Grp., 795 F.Supp.2d 770, 790 (N.D.Ill.2011) (citing Pollstar v. Gigmania, Ltd., 170 F.Supp.2d 974, 981 (E.D.Cal.2000)); see also Mark A. Lemley, Terms of Use, 90 MINN. L.REV. 459, 477 (2006) ("Court may be willing to overlook the utter absence of assent only when there are reasons to believe that the [website user] is aware of the [website owner's] terms."); Note, Ticketmaster Corp. v. Tickers.com, Inc.: Preserving Minimum Requirements of Contract on the Internet, 19 BERKELEY TECH. L.J. 495, 507 (2004) ("[S]o far courts have held browsewrap agreements enforceable if the website provides sufficient notice of the license."). Where, as here, there is no evidence that plaintiffs had actual knowledge of the agreement, "the validity of a browsewrap contract hinges on whether the

website provides reasonable notice of the terms of the contract." Van Tassell, 795 F.Supp.2d at 791 (citing Specht, 306 F.3d at 32).

Here, the Terms of Use hyperlink can be found on every Zappos webpage, between the middle and bottom of each page, visible if a user scrolls down. (Carton Decl. Ex. 1 (# 10–9).) For example, when the Zappos.com homepage is printed to hard copy, the link appears on page 3 of 4. (Id.) The link is the same size, font, and color as most other non-significant links. (Id.) The website does not direct a user to the Terms of Use when creating an account, logging in to an existing account, or making a purchase. (Id.; Carton Decl. Ex. 2 (# 10–10), Ex. 3 (# 10–11), Ex. 4 (# 10–12)., Ex. 5 (# 10–13); Ex. 6 (# 10–14), Ex. 7 (# 10–15).) Without direct evidence that Plaintiffs click on the Terms of Use, we cannot conclude that Plaintiffs ever viewed, let alone manifested assent to, the Terms of Use. The Terms of Use is inconspicuous, buried in the middle to bottom of every Zappos.com webpage among many other links, and the website never directs a user to the Terms of Use. No reasonable user would have reason to click on the Terms of Use, even those users who have alleged that they clicked and relied on statements found in adjacent links, such as the site's "Privacy Policy." This case is therefore factually similar to cases that have declined to enforce arbitration clauses, such as Hines v. Overstock.com, wherein the Court refused to enforce an arbitration provision because the plaintiff "lacked notice of the Terms and Conditions because the website did not prompt her to review the Terms and Conditions and because the link to the Terms and Conditions was not prominently displayed so as to provide reasonable notice of the Terms and Conditions." 668 F.Supp.2d 362, 367 (E.D.N.Y.2009) aff'd 380 Fed.Appx. 22 (2d Cir.2010); see also Specht, 306 F.3d at 32 ("[A] reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms."); Van Tassell, 795 F.Supp.2d at 792 (declining to enforce arbitration provision where "a user only encounters the Conditions of Use after scrolling to the bottom of the home page and clicking the 'Customer Service' link, and then scrolling to the bottom of the Customer Service page or clicking the 'conditions of Use, Notices & Disclaimers' link located near the end of a list of links on the page."); Koch Indus., Inc. v. Does, No. 2:10CV1275DAK, 2011 WL 1775765, at *24–25 (D.Utah May 9, 2011) (finding there was no manifested assent where the "Terms of Use ... were available only through a hyperlink at the bottom of the page, and there was no prominent notice that a user would be bound by those terms."); Cvent, Inc. v. Eventbrite, Inc., 739 F.Supp.2d 927, 936–37 (E.D.Va.2010) (declining to enforce "Terms of Use" where "link only appears on event's website *1065 via a link buried at the bottom of the first page" and "users of event's website are not required to click on that link, nor are they required to read or assent to the Terms of Use in order to use the website or access any of its content."). We therefore agree with the Hines court: "Very little is required to form a contract nowadays—but this alone does not suffice." 668 F.Supp.2d 362, 367. Where, as here, there is no acceptance by Plaintiffs, no meeting of the minds, and no manifestation of assent, there is no contract pursuant to Nevada law.

…

V. Conclusion

A court cannot compel a party to arbitrate where that party has not previously agreed to arbitrate. The arbitration provision found in the Zappos.com Terms of Use purportedly binds all users of the website by virtue of their browsing. However, the advent of the Internet has not changed the

basic requirements of a contract, and there is no agreement where there is no acceptance, no meeting of the minds, and no manifestation of assent. A party cannot assent to terms of which it has no knowledge or constructive notice, and a highly inconspicuous hyperlink buried among a sea of links does not provide such notice. Because Plaintiffs did not assent to the terms, no contract exists, and they cannot be compelled to arbitrate. In any event, even if Plaintiffs could be said to have consented to the terms, the Terms of Use constitutes an illusory contract because it allows Zappos to avoid arbitration by unilaterally changing the Terms at any time, while binding any consumer to mandatory arbitration in Las Vegas, Nevada. We therefore decline to enforce the arbitration *1067 provision on two grounds: there is no contract, and even if there was, it would be illusory and therefore unenforceable.

IT IS, THEREFORE, HEREBY ORDERED that Defendant Zappos.com, Inc.'s Motion to Compel Arbitration and Stay Action (# 3) is DENIED.

Footnotes

1. Plaintiffs have named both Amazon and Zappos as Defendants. Defendants, however, contend that Amazon does not do business as Zappos.com and is therefore incorrectly named.

…

5. While which state's law should apply is not entirely clear given the plethora of states from which these cases arise, the parties apply Nevada law in their respective filings, and the Court will do the same.

Common Law Protections of Individuals' Rights in Personal Information

William J. Fenrich
Fordham Law Review
Volume: 65
Starting Page: 951
December, 1996

Introduction

As you live your life you leave an explicit and revealing trail of electronic footprints.[1] Simply by being born;[2] getting married;[3] having a child;[4] or dying;[5] purchasing something with a check or a credit card;[6] subscribing to a magazine;[7] calling an 800 or 900 number;[8] using ***952** a discount card at a supermarket;[9] or applying for a driver's license;[10] you leave a record of where you were and what you did, and the holder of that record is free to do with it whatever he or she pleases. These transactional footprints have value because they can provide businesses a glimpse of your life that might indicate your receptiveness to products or services these businesses offer.[11] While each record has some individual value, the information develops its greatest value, and greatest power, when the individual pieces are gathered and layered on top of one another, creating a detailed profile of who you are and what you do.[12] This 'personality profile'[13] allows marketing companies to make numerous assumptions about your interests and spending habits, thereby enhancing these marketers' ability to target solicitations to those people most inclined to respond.[14] As a result, you would inevitably find yourself categorized on one or more of the thousands of lists that are bought, rented, or sold each day.[15] This is particularly true of persons meeting certain identifiable and sensitive ***953** characteristics.[16] The breadth and specificity of these lists can be astounding.[17]

Many Americans believe these practices to infringe upon their right to privacy. Recent cases demonstrate the scope and type of privacy violations emanating from unauthorized dissemination of personal information.[18] In one case, a woman from Burbank, California ordered ***954** a maternity catalog after she became pregnant.[19] Not surprisingly, she was soon bombarded with 'more catalogs, baby-product samples, calls from baby photographers and diaper services.'[20]There was one problem with these offers, however: the woman's pregnancy ended with a miscarriage. She made repeated phone calls requesting that the product manufacturers stop soliciting her.[21] When she explained to the telephone solicitors what had happened to her pregnancy, they often hung-up on her. Her requests unheeded, the solicitations continued, and included birthday wishes and baby product offers which reminded the woman of her lost pregnancy.[22] She became so upset that her husband had to open all of the mail and answer all phone calls to the house. Finally, after almost two years of unanswered requests, she sent a letter to all the solicitors, as well as to the major list brokers, explaining what had happened and threatening legal action if the solicitations did not cease. The 'enticing offers' finally subsided.[23]

In another example, an eighty-three year-old woman was targeted by marketers who learned from her purchases that she was elderly and lived alone.[24] Vulnerable to ostensibly 'personal'

calls from marketers who asked for her by name, the woman was induced to purchase many items for which she had no use but was made to think she needed.[25]

***955** It seems that the only definite way to protect personal privacy[26] is to leave no transactional trace as you live your life;[27] an exceedingly difficult task in a society becoming increasingly automated and computerized.[28] Indeed, most Americans would be surprised to learn the scope of businesses' use of personal information.[29]

But many Americans are aware of the increased unauthorized use of personal information. Public opinion polls and privacy surveys seem to indicate the widespread belief of many Americans that they cannot control information about their personal lives.[30] Many persons believe that they possess an innate right to control personal information,[31] but also feel that they have lost the ability to control that information.[32] Not surprisingly, most Americans seek to gain more control over the dissemination of personal information.[33]

***956** In contrast to the concerns of these individuals lie the interests of the direct marketing industry. Some estimates find that direct marketing in 1995 led to as much as $600 billion in sales of goods and services,[34] and employed over eighteen million people.[35] The annual market for mailing lists alone, without factoring in sales attributable to their use, has been estimated at approximately $3 billion.[36] Additionally, the American Telemarketing Association asserts that telephone salespeople made $159 billion in consumer sales in 1995.[37]

The balance of power between the direct marketing industry and the consumers upon whose information it depends is currently tilted strongly in favor of the marketers. Despite the apparent public concern over unauthorized uses of personal information, it remains legal to disseminate personal information without first obtaining the consent of the subject.[38] Individuals currently have no right to be informed of the number, names, or types of lists that contain their names,[39]nor do they have a right to have their names removed from these lists.[40] In fact, the direct marketing industry,[41] which has perhaps the largest stake in continued non-regulation of personal information sales, is not subject to any regulation at all.[42]

Against this backdrop of competing interests, attempts to vindicate individuals' rights in personal information have been made in both judicial and legislative forums. In the courts, as described in part IV, ***957** at least three cases have been brought claiming that the unauthorized sale of consumer information violates the appropriation tort.[43] Not one has been successful.

In addition to these judicial attempts, many commentators have advocated legislation that would grant individuals legal rights in their personal information.[44] These commentators argue that the legislature is better equipped than a court to establish such a right, which would require that any person or institution must obtain the affirmative consent of a data-subject before disseminating to third-parties that data-subject's name, address, and/or telephone number.[45] Actual legislative proposals have been introduced in a number of state legislatures ***958** over the past year.[46]Again, not one, however, has been successful.

…

I. Collection and Dissemination of Personal Information

As described in the Introduction, businesses' ability to collect, process, store, and disseminate personal information is significant. This part explains the nature of the personal information industry and reviews accumulating evidence that American consumers are becoming increasingly concerned about their perceived loss of control over personal information.

Almost all day-to-day consumer and business transactions leave some sort of an electronic record.[47] Information about individuals is collected by computers during transactions and subsequently stored in computer databases.[48] Sources of information include: credit card transactions,[49] mortgage records,[50] magazine subscription information,[51] birth records,[52] warranty cards,[53] point-of-purchase plans,[54] and driver registration records. Driver registration records historically ***960** have been a lucrative source of personal information.[55] For example, the state of Florida has quoted a price of $33 million for a one-time sale of its motor vehicle records database.[56] Because of recent cases where such information was used to advance criminal behavior,[57] however, distribution of such records has become subject to regulation.[58]

Direct marketers place these layers of information on top of one another, and form a profile of the individual that represents some or all of the above factors.[59] This practice results in the creation of an ‘electronic persona,‘[60] and the resulting multi-faceted portrait is aptly known as a ‘personality profile.‘[61] People inadvertently leave traces that create this persona or profile simply by living their lives in an electronic society that forces them to leave electronic footprints almost wherever they go.[62]

***961** While a record of any one factor standing alone has minimal value, the compiled information which paints a comprehensive picture of the individual, enables direct marketers to ‘target‘ their audience and increase response rates on their promotions.[63] This ‘targeting‘ is extremely valuable to the marketers because it increases profits by focusing mailings, decreasing mailing costs, and increasing returns.[64]

Consumers are becoming increasingly aware that businesses gather and use personal information, and that there are occasionally dangerous consequences.[65] Two recent surveys have attempted to gauge Americans' concern over privacy issues. A 1994 Yankelovich Monitor survey found that ninety percent of those polled favored legislation to regulate business compilation of consumer information.[66] Another poll, part of an ongoing series commissioned by one of the ‘Big Three‘ credit reporting bureaus,[67] found that ‘[t]he vast majority of Americans [eighty percent] agree that ‘consumers have lost all control ***962** over how personal information about them is circulated and used by companies.’‘[68] The 1995 numbers reflect a trend in which concern has grown steadily since 1990.[69]

Additionally, a 1991 Time/CNN poll found that ninety-three percent of Americans believe that ‘companies that sell information to others [should] be required by law to ask permission from individuals before making the information available.‘[70] Despite strong claims for regulation in some surveys, the 1995 Equifax survey found that seventy-two percent of the respondents agree that ‘if companies and industry associations adopt good voluntary privacy policies, that would be better than enacting government regulations.‘[71] Respondents to the second poll would back legislation, however, if these voluntary mechanisms were not effective.[72] Evidence suggests, however, that this self-regulation has not been effective.

As mentioned above, the direct marketing industry is entirely free from government regulation.[73]This fact is related to its successful lobbying efforts in 1977 which led to Privacy Commission recommendations that the industry be allowed to police itself.[74]

…

A. Legislative Enactments

…

Like their federal counterparts, state enactments often target specific areas and fail to provide comprehensive privacy protection. The level of protection varies from state to state, but generally protection exists in industry-specific settings.[135] Virtually all states recognize the ***971** right of privacy in some form, either at common law or by statute.[136] California increased its protection in 1993 when it passed a bill requiring credit card issuers to notify their customers that their names and addresses may be sold to direct marketers;[137] the law also mandates that these companies give customers a way to opt-out of having their names sold or rented.[138] Although this statute is a positive legislative step, there is evidence that it is misdirected because credit card companies are not very active in the reselling of customer data.[139] It is also questionable whether such protection would be successful on a broader scale, given the ill-fated introduction in 1996 of legislation that would vest individuals with rights in personal information.[140]

B. The Right to Privacy

Questions about control over personal information traditionally have been conceived under the privacy rubric.[141] It is therefore useful to look to that right as a potential source of protection against the unauthorized dissemination of personal information. Currently, this area of law does not vest individuals with a right to prevent unauthorized dissemination of personal information. This section discusses the current state of the right to privacy and examines how this doctrine might apply to unauthorized sales of personal information. It concludes by noting one court's observation that legislatures, rather than courts, should address the issue of individuals' rights in personal information.

…

American courts addressing privacy between private persons have been influenced largely by the work of Professor Prosser. In his 1960 law review article, Privacy,[148] Professor Prosser surveyed cases decided under the privacy rubric, and argued that the right to privacy was in fact four separate torts:[149] intrusion upon seclusion;[150] public ***973** disclosure of private facts;[151]false light;[152] and appropriation of one's name or likeness for commercial gain.[153] The Restatement (Second) of Torts has acknowledged these distinctions,[154] and most states enforce some or all of the causes of action.[155]

Of these four torts, it appears that the appropriation tort[156] is the most likely to provide protection against unauthorized dissemination of personal information.[157] This tort enjoys recognition in virtually every state through statute or case law.[158] Plaintiffs in three separate cases have attempted to use the appropriation tort to enjoin direct- ***974** marketing related sales of their names and addresses,[159] but none of these attempts has been successful. The first case, Shibley v. Time, Inc.,[160] which was decided on questionable grounds,[161] is particularly notable for the manner in which the court suggested that the legislature, rather than the court, is competent to

consider the issue in the first place. After stating that Time Magazine was not liable under a privacy theory for selling subscriber lists without first obtaining the consent of the subscribers, the court stated that it was not competent ‘to create a specific right which is not recognized at common law.‘[162] It continued to note that:

> The founders of our nation constitutionally set up a government composed of three branches--the legislative, executive and judicial. It is improper for one to invade the province of the other. This is a case peculiarly within the province of the legislative branch and it would be improper for the judicial branch to usurp the legislative function. The judicial branch may interpret the laws enacted by the legislative branch but it may not legislate, and that is what would be required if the plaintiff is to succeed here.[163] In this regard, the Shibley court raised an important issue: what institution--a court or a legislature--is competent to decide whether individuals should be vested with legal rights in personal information? Part III addresses this threshold question of institutional competence.

…

IV. A ‘Reform’ Minded Approach to Judicial Protection of Personal Information

[T]he Reform Model advocates an active lawmaking role for the judiciary in situations where interest group pressure distorts legislative consideration of an issue. This part demonstrates that interest group pressure has, in fact, distorted legislative consideration of individuals' rights in personal information. Accordingly, it argues ****986*** that courts should face the issue on its merits. After examining three cases in which courts failed to act in the Reform Model sense and refused to make what would have been principled extensions of existing privacy doctrine, it demonstrates the legal basis upon which these and other courts could extend privacy protection to rights in personal information. Finally, this part presents privacy cases in which courts acted in a ‘reform‘ sense to develop the very right to privacy which now forms the basis upon which courts should, in light of social and technological change, protect individuals' rights in personal information. In this manner, this part demonstrates that courts expanding common law privacy protection to personal information will in fact be acting consistently with the reasoned development of privacy doctrine throughout the twentieth century.

A. Interest Group Effects on Personal Information Legislative Proposals

[T]he Reform Model demonstrates that interest groups distort legislative processes, especially in situations where they block, rather than promote, legislative activity. Accordingly, because they would be blocking rather than advocating legislation, interest groups' power would be particularly strong with regard to proposals to vest individuals with rights in personal information.[235] Recent examples in fact bear out the difficulties in this arena.

A stark example of legislative process failure in the context of individuals' rights in personal information was recently played out in the California legislature. State Senator Steve Peace, Chairman of the California Senate Committee on Energy, Utilities and Communications introduced a bill that would have vested in individuals an enforceable right in their personal information.[236] The pertinent portion of the bill provided that ‘[n]o person or corporation may use or distribute for profit any personal information concerning a person without that person's

written consent. Such information includes, but is not limited to, an individual's credit history, finances, medical history, purchases, and travel patterns.'[237] The bill contained the following legislative finding concerning the California right to privacy:

Advances in technology have made it easier to create, acquire, and analyze detailed personal information about an individual; ***987** [p]ersonal information, including information about a person's financial history, shopping habits, medical history, and travel patterns, is continuously being created; [t]he unauthorized use of personal information concerning an individual is an infringement upon that individual's right to privacy.[238] The bill was proposed in reaction to the proliferation of online services and their capacity to gather and store personal information, but was drafted to cover personal information gathered and stored in any manner.[239] Further, the bill was proposed against the backdrop of the California Constitution which provides that all people have certain inalienable rights, including the right to privacy.[240] Senator Peace called the bill 'a simple implementation of California's existing constitutional protection of privacy.'[241]

When the bill was introduced in February, 1996, there were predictions that the bill would not be 'likely to move out of committee due to corporate opposition which has mustered a formidable lobbying presence.'[242] A committee consultant who helped draft the bill explained how interest groups dominate consideration of such a measure:

The organized constituency in Sacramento [California's capital] is the larger business interests and they are against the bill. . . . There aren't any organized constituencies in support of the bill. They're just ordinary people. They send us mail and tell us, 'We agree with you completely,' but they are not organized in any effective way up here. You can't counterbalance the opposition, and because of that it will be a tough bill to [pass].[243] Indeed, privacy commentators noted that the legislation 'will be lobbied to the max--ferociously. . . . The legislation . . . does not have an easy road ahead of it.'[244] Senator Peace himself understood from the start that his bill faced an uphill battle,[245] but nonetheless desired to get the fight underway: 'Every day those computers keep cranking out of our control, more information is absorbed, more mistakes are made, and the task of bringing things back under control just gets bigger and bigger.'[246]

These predictions were borne out in practice. Soon after it was introduced, the bill was 'bombarded' by commercial enterprise interest ***988** groups, led by the large national credit reporting agencies.[247] A compromise was forced, and now the bill merely creates a task force, comprised of three Senators and three Assemblymen, charged with evaluating how current California law conforms with the privacy protection mandate of the state constitution.[248] The task force's report is due in March 1998, in time for that year's legislative session.[249] There was minimal press coverage of the initial proposal, and no coverage of the compromise that resulted after commercial interests exerted pressure.[250]

This experience is common with regard to consumer legislation.[251] Similar proposals introduced in the New Jersey[252] and New York[253] state legislatures in early 1996 were also expected to 'languish[ ] in committee.'[254] Massachusetts state legislators have announced their intention to introduce a similar proposal in their 1997 session, which commences in January.[255]

The role of interest groups in determination of personal information issues is not new. … Congress in 1977 considered the privacy implications of mailing list sales, and held hearings on the issue. The direct marketing industry made a strong showing at these hearings, and their testimony and proposals pervade the Commission's report.[256]

Direct-marketers testified at length to the 1977 Privacy Commission about the economic necessity of mailing list profiling, and sought to convince them that the industry should be left to police itself because the industry itself would want to discriminate among consumers with varying levels of privacy concerns. '[T]he best direct-mail campaign is the one that mails the least. This is a business necessity. . . . A piece of mail to an individual who doesn't want to buy is wasted, and to ***989*** direct mailers the elimination of this kind of waste is absolutely essential.'[257] Self-regulation has not proven successful, however.[258] Additionally, the Fair Credit Reporting Act's current inability to adequately safeguard personal privacy is attributable to provisions that were inserted at the behest of an aggressive commercial interest lobby.[259]

Although these events cannot conclusively prove that interest groups will always defeat meaningful consideration of proposals to establish legal rights in personal information, they do shed clear light on the difficulty of passing such proposals in the face of organized and financially powerful interest groups.

B. Unsuccessful Attempts To Apply the Appropriation Tort To Prevent Nonconsensual Dissemination of Personal Information

Plaintiffs in three separate cases have unsuccessfully attempted to apply some form of the appropriation tort to stop unauthorized dissemination of personal information. This part examines these decisions and suggests that a legitimate basis exists for expanding existing common law privacy doctrine to protect against unauthorized dissemination of personal information.

1. Shibley v. Time

In Shibley v. Time, Inc.,[260] a 1977 decision that has been widely criticized,[261] plaintiffs sought an injunction requiring Time Magazine to obtain subscriber consent before selling subscription lists.[262] The Ohio Court of Appeals held that the magazine's sale of the lists to direct mail advertisers without first obtaining the subscribers' consent was not an invasion of privacy, even if the practice amounted to sale of 'personality profiles,' because the information was used only to determine what type of advertisement would be sent.[263]

The plaintiffs attempted to fit their claim within the 'appropriation' branch of the right to privacy, which, under Ohio common law, prohibits the 'unwarranted appropriation or exploitation of one's personality.'[264] Plaintiffs argued that defendants' sale of subscription lists ***990*** amounted to sales of 'personality profiles,' which subjected the subscribers to solicitations from direct mail advertisers.[265] Plaintiffs then, somewhat vaguely, alleged that this practice amounted to an invasion of privacy that was not consented to nor made part of the original subscription contract.[266] The court dismissed this argument on two questionable grounds. First it held that the appropriation tort only applies where the plaintiff's name or

likeness is displayed to the public.[267] This argument is suspect, however, because it is arguable whether, once the information is spread to a multitude of third-parties, it might be considered ‘displayed‘ for the purposes of the rule; also, not all jurisdictions require publicity as such in misappropriation cases.[268]

Second, the court held that plaintiffs have no expectation of privacy in their mailboxes.[269] In so holding, the court looked to the Ohio legislature's provision allowing third parties to compile and sell lists of the names and addresses of motor vehicle registrants. The court held that this act implied that an individual's rights of privacy are not compromised by sale of personal information.[270] The court also relied upon Lamont v. Commissioner of Motor Vehicles,[271] a federal case that found constitutional a New York statute that authorized the New York State Department of Motor Vehicles to sell driver registration lists.[272] In dismissing the complaint, the Lamont court used the following language, upon which the Shibley court relied heavily:

> ***991** The mail box, however noxious its advertising contents often seem to judges as well as other people, is hardly the kind of enclave that requires constitutional defense to protect ‘the privacies of life.’ The short, though regular, journey from mail box to trash can . . . is an acceptable burden, at least so far as the Constitution is concerned.[273]

Shibley's reliance on Lamont is incorrect for two reasons. First, Lamont dealt with a constitutional right of the individual to privacy as against the state; it did not address relations between private actors. This distinction is clear in cases and the literature.[274] Second, the Shibley court focused only on the end-use of the information, citing precedent that mail solicitation does not violate individuals' privacy. Regardless of whether or not the end-use may infringe on privacy rights, the end-use is not the violation in these cases. Rather, it is the sale of the information to the end-users in the first place that constitutes the tortious appropriation of the plaintiffs personality.[275]Accordingly, whether there is an expectation of privacy in the mailbox is irrelevant to the claim asserted by plaintiffs in Shibley.[276]

Finally, as discussed above, the court noted its incompetence to even handle the question presented in the first place.[277]

2. Dwyer v. American Express

A recent Illinois case, Dwyer v. American Express Co.,[278] reconsidered the sale of personal information and relied heavily upon Shibley. Similar to Shibley, the Dwyer complaint alleged that American Express, through its practice of compiling and selling lists of cardmembers names and addresses arranged by ‘personality profiles,‘ invaded the cardmembers' privacy and violated the Illinois Consumer Fraud statute.[279] The Illinois Appeals Court affirmed the trial court's ***992**grant of defendant's motion to dismiss for failure to state a claim.[280] The Illinois Supreme Court denied certiorari.[281]

Plaintiffs made three unsuccessful claims. The first was a privacy claim fashioned under the intrusion upon seclusion tort.[282] Plaintiffs' second claim was fashioned under Illinois' Consumer Fraud statute.[283] The plaintiffs' third claim was brought under the appropriation tort, recognized at common law in Illinois.[284] The court cited the Restatement's position that the purpose of the

tort is to protect the ‘interest of the individual in the exclusive use of his own identity, in so far as it is represented by his name or likeness.‘[285] Defendant argued rental of the information did not interfere with plaintiff's ‘exclusive use of his own identity‘; the names themselves had no value; and if there is in fact value in the list, defendants created such value through their efforts to compile the information and make aggregate lists.[286] Plaintiffs ***993*** countered by citing cases finding appropriation even where the name or likeness is used for a non-commercial purpose.[287]

The court, however, looked no further than Shibley to decide the case.[288] Without explaining Shibley's rationale for dismissing the appropriation claim, the court dismissed plaintiffs' claim on the ground that there is no value in one name.[289] The court ruled that the defendants created the valuable product when they analyzed the cardmember information and compiled aggregate lists of cardmembers' names.[290]

The Shibley court, however, based no part of its decision on the relative value of individual names versus a compiled list of names. Accordingly, the Dwyer court based its dismissal of the appropriation claim on precedent that does not exist. Despite Dwyer's citation to Shibley, no precedent supports its argument that there can be no appropriation because there is no value in a single name.

…

Conclusion

…

Disproportionate interest-group pressure distorts the legislative process and gives courts the responsibility to address the personal information issue on its merits, so as to weaken the legislative inertia amassed against meaningful consideration of proposals to grant individuals rights in personal information. This jurisprudential model can liberate the lawmaking capabilities of our republican government without providing judges with unrestrained power, because any court-created rule is always subject to review, and even veto, by the legislature.

Footnotes

1. See Joel R. Reidenberg, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 Iowa L. Rev. 497, 517 (1995) [[[hereinafter Reidenberg, Setting Standards] (describing how the direct marketing industry collects ‘discrete bits of personal information from many sources‘); Michael W. Miller, Hot Lists: Data Mills Delve Deep to Find Information About U.S. Consumers: Folks Inadvertently Supply It by Buying Cars, Mailing Coupons, Moving, Dying, Wall St. J., Mar. 14, 1991, at A1 (‘You go through life dropping little bits of data about yourself everywhere.... Most people don't know that there are big vacuum cleaners sucking it up.‘ (quoting privacy advocate Evan Hendricks, editor of Privacy Times, a Washington, D.C., monthly)); Mary Zahn & Eldon Knoche, Electronic Footprints: Yours Are a Lot Easier to Track Than You May Think, Milwaukee J. Sentinel, Jan. 16, 1995, at 1A. Zahn and Knoche describe the results of their findings as follows:
Write a check and somewhere a computer may log in your name. Buy an expensive dinner with a credit card and a databank may register you as an upscale consumer. Apply for a driver's license and anyone with a few bucks can know your age and address. Send for a video and someone will know your taste in movies. Use a discount card at a supermarket and the can of tuna fish you bought leaves an electronic fingerprint. Even breathing can be a spectator sport for your medical records may end up in a Boston information bank. As you are born, go to school, get a job, have a family, raise your kids, retire and die, nearly everywhere you go and everything you do leaves computer footprints behind. And in some cases,

governmental agencies, which you probably thought would be sympathetic to protecting your privacy, work hand in hand with these merchants by making available to them intimate facts about your life. And it's all legal.
Id.
2. Zahn & Knoche, supra note 1, at 1A.
3. Miller, supra note 1, at A8.
4. See id. (noting marketing efforts targeted at women intending to have children); R.J. Ignelzi, Mail and Telejunk: U.S. Marketers Have Your Number: Your Age and Shoe Size, Too, San Diego Union-Trib., July 4, 1995, at E1.
5. See Miller, supra note 1, at A8 (noting statement by president of marketing firm that collects information on recent deaths, who stated that '[d] eath has always been a negative life style change nobody thought could be sold, but I differ ... I think it's a very good market').
6. Zahn & Knoche, supra note 1, at 1A.
7. See Avrahami v. U.S. News & World Rep., Inc., No. 96-203, slip op. at 10-11 (Cir. Ct. Arlington County June 13, 1996).
8. Zahn & Knoche, supra note 1, at 1A.
9. Id.
10. Id. For a discussion of state sales of driver registration records, see infra notes 55-58 and accompanying text.
11. These discrete bits of information are traded widely among catalog and magazine publishers. For example, on the assumption that subscribers to U.S. News & World Report might be inclined to subscribe to Smithsonian magazine, the latter rented from the former a list of the names and addresses of U.S. News subscribers. This activity spawned a lawsuit by a U.S. News subscriber who argued that U.S. News unlawfully appropriated his name and likeness for commercial gain. See Avrahami, No. 96-203, slip op. at 7-8. For a more detailed discussion of the Avrahami case, see infra notes 291-97 and accompanying text.
12. See Zahn & Knoche, supra note 1, at 1A ('Bits of personal and financial facts about you, valuable in individual pieces, become more profitable as chunks of data are overlaid on each other. Layers and layers of easily acquired information are merged into a profile that is treasured by magazines, car dealerships, banks, insurance companies and anyone else who wants to market a product to you or determine that you are a poor health or credit risk.'); see also Reidenberg, Setting Standards, supra note 1, at 516-23 (detailing the profiling techniques employed by direct marketing companies); Jonathan Berry, Database Marketing: A Potent Tool for Selling, Bus. Wk., Sept. 5, 1994 at 56 (describing how information is collected and combined 'into the database maw' to generate complex profiles of consumers and their interests).
13. 'Personality profiles' are those records, lists, or representations that combine multiple pieces of personal information about a given 'data subject.' See Reidenberg, Setting Standards, supra note 1, at 517 ('By cross-referencing numerous items of personal information, individual profiles are developed. These profiles may consist of a single characteristic, such as subscribers to Penthouse or denture adhesive buyers. They may also consist of a more complete set of characteristics.'). A 'data subject' is merely the individual whose personal information is gathered. See infra note 18 (detailing legislative proposals that define 'data subject').
14. Zahn & Knoche, supra note 1, at 1A.
15. At least 10,000 lists of data about individuals are available for rent. National Telecommunications and Information Administration, Inquiry on Privacy Issues Relating to Private Sector Use of Telecommunications-Related Personal Information, 59 Fed. Reg. 6842, 6842 (1994) [hereinafter NTIA Inquiry].
16. Zahn & Knoche, supra note 1, at 1A ('Troubling to many is the sale of lists of people who meet sensitive and personal criteria. Any lesbian or a diabetic has a good chance of being on a list. A Jew has an excellent chance of making some marketing list.').
According to a former head of a Federal commission charged with investigating personal privacy

concerns, ‘[w]ithout our knowledge we are profiled and placed on many specialized lists, whether we like it or not.... You could be classified as a foreign policy hawk, affluent ethnic professional, black activist, person who frequents the dice table. You don't know what lists you are on.‘ Id. (quoting David F. Linowes, former chairman of the U.S. Privacy Protection Study Commission).
17. For example, lists including the names of the following Americans have been sold by list brokers: more than 300,000 men who called various 800/900 phone fantasy numbers; 55,912 gay and lesbian magazine subscribers; 5000 women who responded to an 800 phone number offering information and samples of adult diapers (this list sold for $270); and 82,000 men 55 and older who sought help for impotency at a medical clinic. Id.
Additionally, one company, which deems itself the world's leading broker and manager of Jewish lists, claims it ‘can identify and mail to 85% of the 2.6 million Jewish households in the United States.‘ Id. As the authors of this newspaper article note, ‘[g]enerally, these lists are rented for one-time use only by list brokers who are the real estate agents of the information industry.‘ Id.
18. For the purposes of this Note, ‘personal information‘ is information that in any way concerns or reflects the personality of an individual. A similar definition is ‘information ... gathered, stored, or disseminated in ways that make likely its association with particular individuals.‘ Laurence H. Tribe, American Constitutional Law, ss 15-17, at 967 (1978).
The scope of the definition is not as important as whether the information has value to those who seek to appropriate it. California has a statute that regulates governmental collection, transmission, and sale of personal information. Cal. Civ. Code s 1798.3 (West. Supp. 1996). While this Note concerns trade by private parties of personal information, California's definition helps delineate the possible scope of the definition. It reads:
The term ‘personal information‘ means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.
Id.
Additionally, the statute exempts from its scope dissemination of newsworthy information: ‘The term ‘commercial purpose’ means any purpose which has financial gain as a major objective. It does not include the gathering or dissemination of newsworthy facts by a publisher or broadcaster.‘ Id. s 1798.3(j).
A broader definition proposed by the European Community includes ‘any information relating to an identified or identifiable natural person (‘data subject’).‘ James R. Maxeiner, Business Information and ‘Personal Data‘: Some Common-Law Observations About the EU Draft Data Protection Directive, 80 Iowa L. Rev. 619, 619 & n.1 (1995) (citing Article 2(a) of the Commission of the European Communities ‘Amended Proposal for a Council Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data‘ of October 16, 1992, 1992 O.J. (C 311) 38).
An appropriate understanding of personal information is closer to the EC proposal, i.e., any information relating to an identifiable person. In the case of the sale of a magazine subscriber's name, for instance, the actual information that is sold is not only the name and address, but also the subject's association with the seller. In this instance, the information quite literally ‘relates‘ to the ‘identified or identifiable natural person (‘data subject’).‘
19. Ignelzi, supra note 4, at E1.
20. Id.
21. Id.
22. Id.
23. Id.
24. Id.
25. Id. In another case, a woman and her husband, a police officer, worked hard to keep their address secret. They were successful until the woman had her first child; she was immediately inundated with marketing offers personally addressed to her. It turns out that the hospital had sold her name and address

to direct marketers on a list of new mothers. Mark Lewyn, You Can Run, But It's Tough to Hide from Marketers, Bus. Wk., Sept. 5, 1994, at 60.
26. Most discussions of these issues take place under the vague rubric of ‘privacy.‘ See Reidenberg, Setting Standards, supra note 1, at 498 (noting that “[p]rivacy’ serves as a catch-all term‘). Public discourse concerning businesses' dissemination of personal information is usually couched in privacy terms. See, e.g., Louis Harris & Associates & Alan F. Westin, 1995 Equifax-Harris Mid-Decade Consumer Privacy Survey (detailing results of survey monitoring consumer attitudes regarding privacy) [hereinafter Equifax Survey]; Yankelovich Monitor, Yankelovich Monitor 1995 Consumer Privacy Survey (same) [[[hereinafter Yankelovich Survey].
27. One commentator proposes a viable, albeit drastic, strategy: ‘Pay cash. Avoid credit. Don't sign up for government programs. Walk, don't drive. Live under a rock. In short, for most ordinary people, there is no way [to] keep yourself off these lists.‘ Stephen Phillips, Never Mind Your Number--They've Got Your Name, Bus. Wk., Sept. 4, 1989, at 81.
28. Jay Greene, Eluding Their Gaze: The Way to Protect Personal Info Is to Leave No Trace. But Remember-The Rules Aren't in Your Favor, Orange County Reg., Apr. 25, 1996, at C1 (‘The idea of becoming a hermit may seem a bit rash. But as Corporate America continues to whittle away at your privacy, the only way to protect personal information is to leave no trace.‘).
29. ‘Most Americans have no idea of the scope of record-keeping.... They would be surprised at how easy it is for others to obtain information the individual assumes is confidential.‘ Zahn & Knoche, supra note 1, at 1A (quoting statement made to Congress by David F. Linowes, former chairman of the U.S. Privacy Protection Study Commission).
30. See Equifax Survey, supra note 26, at 17-33, 61 (detailing results of survey monitoring consumer attitudes regarding privacy); Yankelovich Survey, supra note 26, at 10-20.
Alan Westin, a professor at Columbia and author of an important book on privacy, Privacy & Freedom (1967), consulted on the Equifax survey. He concluded that the survey results indicated strong concern about the use and dissemination of personal information. Equifax Survey, supra note 26, at 9.
31. See J. Thomas McCarthy, Melville B. Nimmer and the Right of Publicity: A Tribute, 34 UCLA L. Rev. 1703, 1711 (1987) (‘[N]othing is so strongly intuited as the notion that my identity is mine--it is my property, to control as I see fit.‘).
32. See Equifax Survey, supra note 26, at 23 (‘The vast majority of Americans (80%) agree that ‘consumers have lost all control over how personal information about them is circulated and used by companies.’‘); Yankelovich Survey, supra note 26, at 18 (noting that Americans are feeling more protective of their privacy in 1995 than they did in the early 1990s).
33. See Claudia Montague, Private Ayes, Marketing Tools Magazine, Jan. 1996, at 1 (citing ‘alarming‘ figures in Yankelovich survey suggesting that nine out of ten Americans favor legislation to regulate business use of consumer information).
34. See Robert J. Posch, The 25-Year Privacy Debate Has an Institutional Memory, Direct Mkt., Apr. 1, 1996, 2 (citing estimates by the Direct Marketing Association (“DMA”) that place the 1995 volume of sales generated by the direct marketing industry at $600 billion).
35. Julian Beltram, Homeowner's Suit over Junk Mail Turns Him into Folk Hero: Payment Demanded for Use of His Name, Vancouver Sun, Nov. 6, 1995, at A6 (estimating that 18.2 million persons are employed by the direct marketing industry).
36. NTIA Inquiry, supra note 15, at 6842.
37. Richard Higgins, Natick Consumer Fed Up at Being Dialed Up; Woman Spurs Bill to Curb Sales of Phone, Address Lists, The Boston Globe, Sept. 1, 1996, at 1.
38. Greene, supra note 28, at C13 (‘[R]ight now the deck is stacked in the favor of businesses. Williams-Sonoma, for example, is under no obligation not to collect transactional data about what you buy and sell it to others. ‘ (quoting Christine Varney, a commissioner of the Federal Trade Commission)).
39. Zahn & Knoche, supra note 1, at 1A (‘Those lists are intended to help direct marketers target customers. Legally, consumers do not have to give permission to have their names sold, nor do they have to be notified of the lists they are on.‘).

40. See Privacy Protection Study Comm'n, Personal Privacy in an Information Society 147 (1977) [hereinafter Privacy Comm'n].
41. The direct marketing industry is represented in its lobbying efforts by the DMA. Established in 1917, the DMA is the "oldest and largest trade association for nonprofit and business organizations using direct marketing to reach their customers, members, and prospects." Children's Privacy: Hearings Before the Subcomm. on Crime of the House Comm. on the Judiciary, 104th Cong., 2d Sess. (1996) [hereinafter Children's Privacy Hearings] (testimony of Richard A. Barton, Senior Vice-President for Congressional Relations, Direct Marketing Association). The DMA represents more than 3000 corporations and organizations in the United States and over 600 corporations in forty-seven other nations. Id.
42. Reidenberg, Setting Standards, supra note 1, at 517.
43. See infra notes 157-59 (discussing tort); infra part IV.B (discussing Shibley v. Time Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975), Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995), and Avrahami v. U.S. News & World Rep., Inc., No. 96-203, (Cir. Ct. Arlington County June 13, 1996)).
At least one other commentator has argued that courts should remedy unauthorized sales of personal information, but through recognition of a new tort-based cause of action. See Jonathan P. Graham, Note, Privacy, Computers, and the Commercial Dissemination of Personal Information, 65 Tex. L. Rev. 1395, 1434-38 (advocating creation of tort of commercial dissemination of personal information). Graham suggests that the greatest impediment to legislative privacy protection is the legislature's lack of a coherent understanding of privacy, although he also acknowledges that legislatures, "faced with the task of balancing the uncertain interests of business against the undefined interests of individuals, might yield to business concerns and undervalue personal privacy." Id. at 1424-25.
This Note argues that interest group pressure has, in fact, distorted legislative consideration of proposals to vest individuals with rights in personal information, and further suggests that adequate protection can be achieved through extension of already-existing common law tort doctrine.
44. See, e.g., Joshua D. Blackman, A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector, 9 Santa Clara Computer & High Tech. L.J. 431, 468 (1993) (proposing federal statute tracking European Community Draft Directive on Personal Data Management, Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data, art. 24.1, 1990 O.J. (C 277) 3, 10); Patricia Mell, Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness, 11 Berkeley Tech. L.J. 1, 2 (1996) (proposing federal statute granting individuals property rights in their electronic personas); Steven A. Bibas, Note, A Contractual Approach to Data Privacy, 17 Harv. J.L. & Pub. Pol'y 591, 606-07 (1994) (proposing a statute mandating that all consumer transactions include terms giving consumers an opportunity to either opt-in or opt-out of secondary use of personal information, which would then lead to a deregulated market-based system of personal information management); Scott Shorr, Note, Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment, 80 Cornell L. Rev. 1756, 1818 (1995) (proposing federal statute that would grant individuals property rights in their personal information that would in turn serve as basis for 'personal information contracts').
Bibas's Note eschews a broad regulatory scheme, and focuses primarily on the benefits of an unregulated market in personal information, the dynamics of which would be influenced by society's shared privacy expectations. Bibas, supra, at 606-07.
45. See Blackman, supra note 44, at 468; Mell, supra note 44, at 76-81; Bibas, supra note 44, at 606-07; Shorr, supra note 44, at 1818.
46. The state legislatures of California, New Jersey, and New York have entertained proposals that would restrict commercial dissemination of personal information. See infra notes 236-50 and accompanying text (discussing ill-fated proposals in various state legislatures).
47. See James Greiff, Use of Credit Card Creates Mini-Profile of Consumer, Portland Oregonian, Sept. 13, 1993, at B10 (recounting activities that leave electronic traces); supra note 1 (same).
48. Aryeh S. Friedman, Law and the Innovative Process: Preliminary Reflections, 1986 Colum. Bus. L. Rev. 1, 31 (noting ability of computers to process and cross-reference information quickly, leading to 'creat[ion of] personal profiles of individual data subjects').

49. See Greiff, supra note 47, at B10; Miller, supra note 1, at A8.
50. See Miller, supra note 1, at A1.
51. Id.
52. Id.
53. See Privacy Advocates Warn Against Warranty Cards, Wis. St. J., Dec. 27, 1995, at 4D (noting that although many consumers believe that these cards are necessary to activate warranty protection, filing the card is not necessary for protection in the event that the product is defective).
54. Under ‘point-of-purchase‘ or ‘point-of-sales‘ plans, consumers receive a card with a magnetic stripe; when they make a purchase, they are automatically given credit for all store coupons then in effect and their purchase history is recorded by household. Data Protection, Computers, and Changing Information Practices, Hearings on H.R. 685 Before the Subcommittee on Government Information, Justice, and Agriculture of the House Committee on Government Operations, 101st Cong., 2nd Sess. 86 (1990) (statement of Jerry Saltzberger, Chief Executive Officer of Citicorp's Point-of-Sale (POS) Information Services); see Blackman, supra note 44, at n.1. These plans record tremendous amounts of detailed information, but are entered into on a more consensual basis than the bulk of methods described above.
55. Driver registration records have traditionally been available for public inspection, and many state Departments of Motor Vehicles have prepared lists and sold them to interested direct marketers. Drivers Privacy Protection Act of 1993: Hearings on H.R. 3365 Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103rd Cong., 2d Sess. (1994) (statement of Mary J. Culnan, associate professor, Georgetown University School of Business). Marketers use both registration and drivers' license files to acquire a broad array of personal information. Each type of record has names and addresses; in addition, however, registration files have information on the types and years of cars that people own, and drivers' licenses contain information about age, gender, weight, height, and need for corrective lenses. These data are valuable to marketing profilers in a number of ways. For example, the make and model of an individual's car may allow inferences about that individual's income; the age of the car might signal the likelihood that the owner will soon purchase a new car; and vital statistics, as reflected on a driver's license, might indicate the subject's likelihood of buying a particular good or service. Professor Culnan cites the example of optometrists targeting senior citizens with bad eyesight who live in a certain area. One marketing executive has stated that ‘nothing says more about you than the car you drive.‘ Id.; see also Jeffrey Rothfeder, Looking for a Job? You May Be Out Before You Go In, Bus. Wk., Sept. 24, 1990, at 128 (noting the use of motor-vehicle histories to investigate job applicants).
56. Larry Rohter, Florida Weighs Fees for Its Computer Data: Some See Profits, Others Too High a Price, N.Y. Times, Mar. 31, 1994, at B9.
57. In 1989, actress Rebecca Schaeffer was murdered in the doorway of her California apartment. Her assailant was an obsessed fan who had stalked her for two years; he finally obtained her home address when he hired a private investigator who simply requested the address from the California Department of Motor Vehicles. Ellen Alderman & Caroline Kennedy, The Right to Privacy 325 (1995).
58. In response to a California stalking case in which the murderer found his victim through state motor vehicle records, see id., Senator Barbara Boxer proposed an amendment to the crime bill that would give drivers the opportunity to opt-out of disclosure of information such as height, weight, hair color, eye color, and corrected vision. See Driver's Privacy Protection Act of 1994, 18 U.S.C. ss 2721-2725 (1994); Reidenberg, Setting Standards, supra note 1, at 518 n.105.
59. See Friedman, supra note 48, at 31; Reidenberg, Setting Standards, supra note 1, at 517.
60. Mell, supra note 44, at 3.
61. Id.
62. Id. (‘We have not consciously created such images of our personae. They are a function of the electronic trail of the information we leave in the wake of our use of any service that electronically records and/or stores information concerning our transactions.‘); Zahn & Knoche, supra note 1, at 1A.
63. See Privacy Comm'n, supra note 40, at 126 (‘The key fact to understand about mailing lists ... is that they are almost never free-standing; they are names and addresses of individuals who have some type of association, usually an active one, with a public or private organization.‘).

As Professor Reidenberg observed:
It is probably not commonly known that credit card companies develop lifestyle profiles of card holders, that telecommunications companies track users' calling patterns, that product manufacturers track the habits of individual customers, and that credit reporting agencies also assemble data on household composition (such as marital status of occupants) and on legal disputes involving individuals.
Joel R. Reidenberg, Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?, 44 Fed. Comm. L.J. 195, 205 (1992) [hereinafter Reidenberg, Fortress or Frontier] (citing David Churbuck, Smart Mail, Forbes, Jan. 22, 1990, at 107; Jeffrey Rothfeder, Is Nothing Private?, Bus. Wk., Sept. 4, 1989 at 74, 74-82; Eben Shapiro, MCI Discounts Expected on Numbers Called Often, N.Y. Times, Mar. 18, 1991, at D4).
The Standard Rate and Data Service mailing-list catalog is used widely in the direct marketing industry, and ‘includes lists that reflect religion, sexual orientation, medical information, and political contributions.‘ Judith Waldrop, The Business of Privacy, American Demographics, Oct. 1994, at 46, 49.
64. Direct marketers testified at length to the 1977 Privacy Commission about the economic necessity of mailing list profiling, stating: ‘[T]he best direct-mail campaign is the one that mails the least. This is a business necessity.... A piece of mail to an individual who doesn't want to buy is wasted, and to direct mailers the elimination of this kind of waste is absolutely essential.‘ Privacy Comm'n, supra note 40, at 135 (quoting testimony of Association of American Publishers).
65. See Equifax Survey, supra note 26, at 5 (noting a significant increase in the percentage of respondents believing that ‘technology has almost gotten out of control‘); Yankelovich Survey, supra note 26, at 14.
66. See Yankelovich Survey, supra note 26, at 18; Montague, supra note 33, at 1.
67. The ‘Big Three‘ credit bureaus are Equifax, TRW, and Trans Union. In 1988 these three bureaus held a combined 410 million files on individuals. Jeffrey Rothfeder, Is Nothing Private?, Bus. Wk., Sept. 4, 1989, at 74, 81; see What Price Privacy, Consumer Rep., May 1, 1991, at 356 (estimating that the United States' credit bureaus maintain files on almost 90% of all adult citizens). Annually since 1990, Equifax has commissioned privacy surveys conducted by Louis Harris and Associates. Equifax Survey, supra note 26, at 1.
68. See Equifax Survey, supra note 26, at 23.
69. From 1990 through 1995, the percentage of people agreeing with the statement that they had ‘lost all control over how personal information about them is circulated and used by companies‘ grew steadily from 71% to 80%. Id. at 24.
70. Richard Lacayo, Nowhere to Hide, Time, Nov. 11, 1991, at 34, 36. The poll also found that 88% believe that companies ‘[s]hould ... be required by law to make the information [they collect about individuals] available to individuals so that possible inaccuracies may be corrected.‘ In addition, 90% were found to believe that companies that collect and sell personal information should be prohibited by law from selling information about household income, and 86% believed that companies should be prohibited from selling information about bill-paying history. Finally, 68% were found to believe that the law should prohibit companies from selling information about consumers' product purchases. Id.
71. Equifax Survey, supra note 26, at 10.
72. Id. at 13.
73. Reidenberg, Setting Standards, supra note 1, at 517 (‘[N]o identifiable sectoral law targets direct marketing.‘).
74. See Posch, supra note 34, at 3 (describing success of DMA lobbying efforts); Privacy Comm'n, supra note 40, at 147.
…
135. See generally Reidenberg, Fortress or Frontier, supra note 63, at 227-36 (detailing state statutes addressing the financial services, telecommunications, home entertainment, information services, and insurance industries). For a general overview of state privacy statutes, see Robert E. Smith, Compilation of State and Federal Privacy Laws (1992).
136. For a comprehensive overview of state privacy law, see McCarthy, supra note 155, ss 6.1-.15.
137. Cal. Civ. Code. s 1748.12 (West 1996).

138. Id.
139. Greiff, supra note 47, at B10 (‘The California bill ‘singles out credit card issuers for invasion of privacy attention, when credit card issuers aren't really much of a culprit in this thing’ .... Catalog companies and magazines violate consumer privacy much more often.‘ (quoting Nationsbank spokesman)).
140. See infra notes 236-50 and accompanying text (detailing interest group pressure leading to failure of proposal that would have granted individuals' rights in personal information).
141. See Reidenberg, Setting Standards, supra note 1, at 498 (noting how ‘[p] rivacy serves as a catch-all term‘).
…
148. William L. Prosser, Privacy, 48 Cal. L. Rev. 383 (1960).
149. Id. at 389. The tort previously had been undifferentiated. The First Restatement addressed privacy by stating merely that ‘[a] person who unreasonably and seriously interferes with another's interest in not having his affairs known to others or his likeness exhibited to the public is liable to the other.‘ Restatement of Torts s 867 (1939).
150. Prosser, supra note 148, at 389. The intrusion tort has been characterized as intentional intrusion ‘upon the solitude or seclusion of another or his private affairs.‘ Restatement (Second) of Torts s 652(B) (1977); see, e.g., Pearson v. Dodd, 410 F.2d 701 (D.C. Cir.), cert. denied, 395 U.S. 947 (1969) (extending ‘tort of invasion of privacy to instances of intrusion, whether by physical trespass or not, into spheres from which an ordinary man in a plaintiff's position could reasonably expect that the particular defendant should be excluded‘).
Because it is concerned with plaintiff's activity in obtaining information, this tort's utility in the personal information context is limited to data collection, rather than dissemination. See Reidenberg, Fortress or Frontier, supra note 63, at 222-23 (noting that the intrusion tort ‘does not address other data protection practices such as the storage, use and disclosure of personal information‘).
151. Prosser, supra note 148, at 392. According to the Restatement (Second), this tort applies to the giving of ‘publicity to a matter concerning the private life of another,‘ where such information is not of legitimate concern to the public, and the nature of the disclosure is ‘highly offensive‘ to a reasonable person. See Restatement (Second) of Torts s 652(D) (1977); Reidenberg, Fortress or Frontier, supra note 63, at 223-24; Shorr, supra note 44, at 1779-80. This tort is not likely to apply to unauthorized dissemination of personal information, because any information voluntarily disclosed in the first instance would be removed from its coverage, and the publication requirement is of a magnitude not reached in the course of intercompany personal profile sales. Reidenberg, Fortress or Frontier, supra note 63, at 223-24.
152. Prosser, supra note 148, at 398. The false light tort guarantees one's right to be ‘secure from publicity that places [a] person in a false light before the public.‘ Restatement (Second) of Torts s 652(E) (1977). This tort would not apply to unauthorized dissemination of personal information because the information here is in most cases true, and the tort requires that the information in question be false or erroneous. Further, the tort requires public dissemination, and the intercompany exchange that would most often occur in the context of personal information exchanges would not reach the necessary threshold of publication. See Reidenberg, Fortress or Frontier, supra note 63, at 224-25.
153. Prosser, supra note 148, at 401.
154. See Restatement (Second) of Torts s 652(A) (1977).
155. See generally J. Thomas McCarthy, The Rights of Publicity and Privacy ss 6.1-.3 (1996) (discussing generally the states' adoption of some or all of Prosser's privacy causes of action).
156. The appropriation tort is defined in the Restatement as follows:
Appropriation of Name or Likeness: One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy.
Restatement (Second) of Torts s 652(C) (1977); see also Keeton et al., supra note 147, s 117, at 851-54; Prosser, supra note 148, at 389.
157. See Mell, supra note 44, at 25 (‘The appropriation tort, being a mix of property and privacy concepts, would be the most likely tort to protect the individual's interest in his persona.‘); Reidenberg,

Fortress or Frontier, supra note 63, at 225 (‘[The tort-based] protection against the misappropriation of one's name may offer coverage ... to ban ... dissemination of personal information for commercial purposes without consent.‘); Graham, supra note 43, at 1414 (‘[T]he appropriation tort could be stretched to cover the situation in which an individual profile, instead of a name or likeness, is used by another.‘); Shorr, supra note 44, at 1818 (‘[T]he theory of property underlying the misappropriation tort and the right to publicity provides the strongest legal foundation for the recognition of property rights in personal information.‘).
158. Keeton et al., supra note 147, s 117 at 851-54 (discussing acceptance of privacy appropriation tort); McCarthy, supra note 155 s 6.1 (same).
159. See infra part IV.B (discussing Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975), Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995), and Avrahami v. U.S. News & World Rep., Inc., No. 96-203, (Cir. Ct. Arlington County June 13, 1996)).
160. 341 N.E.2d 337 (Ohio Ct. App. 1975).
161. See infra part IV.B.1.
162. 341 N.E.2d at 340.
163. Id. (quoting Shibley v. Time, Inc., 321 N.E.2d 791, 795 (Ct. C.P. Ohio (1974)).
…
235. Id. (‘[G]roup influence is likely to be strongest when the group is attempting to block rather than obtain legislation ....‘ (citing Schlozman & Tierney, supra note 198, at 314-15, 395-96)).
236. S. 1659, Cal. 1995-96 Reg. Sess. (Feb. 21, 1996) amended Sept. 21, 1996. See Julie Forster, California, Minnesota and New York Lawmakers Push Internet Privacy Bills, West's Legal News, Mar. 15, 1996, at 1310, available in Westlaw 1996 WL 259030 .
237. See Forster, supra note 236.
238. Id.
239. Id.
240. See Cal. Const. art. 1, s 1.
241. Forster, supra note 236.
242. Id.
243. Id. (quoting Randy Chinn, consultant to California Senate Committee on Energy, Utilities and Communications).
244. Id. (quoting Beth Givens, Project Director of the Privacy Rights Clearinghouse at the University of San Diego School of Law).
245. Rep. Steve Peace, Editorial, San Diego Union-Trib., Feb. 21, 1996, at B9 (acknowledging that it would take a long time before his privacy bill is enacted).
246. Id.
247. Telephone Interview with Randy Chinn, consultant to California Senate Committee on Energy, Utilities and Communication (Oct. 11, 1996) [[[hereinafter Telephone Interview].
248. S. 1659, Cal. 1995-96 Reg. Sess. (Feb. 21, 1996), amended Sept. 21, 1996.
249. Id.
250. See Telephone Interview, supra note 247.
251. Forster, supra note 236.
252. The New Jersey proposal, Senate Bill, No. 795, was introduced on February 15, 1996. It sought specifically to regulate sale of mailing lists, and proposed that ‘[n]o person, including any public or private entity, shall rent, sell or otherwise release the names, addresses, or telephone numbers of individuals to any other person for use in commercial solicitation without the prior written or electronic consent of those individuals.‘ S. 795, 207th Leg. (Feb. 15, 1996).
253. Forster, supra note 236.
254. Id.
255. Higgins, supra note 37, at 1. The citizen who motivated her legislator to propose the legislation complained of ‘the widespread attitude that there's nothing we can do about these mailings and calls, that they are somehow part of the air we breathe and the water we drink.‘ Id.

256. See Posch, supra note 34, at 2. As one direct marketing insider describes the effort: ‘DMA leaders taught and sold the Commission ... and set in place the set-piece of self-regulation.‘ Id. at 2-3.
257. Privacy Comm'n, supra note 40, at 135 (quoting testimony of Association of American Publishers).
258. See supra notes 75-92 and accompanying text (detailing ineffective self-regulation in direct-marketing industry).
259. See supra note 121.
260. 341 N.E.2d 337 (Ohio Ct. App. 1977).
261. See Reidenberg, Fortress or Frontier, supra note 63, at 216; Graham, supra note 43, at 1413; Shorr, supra note 44, at 338. For a comprehensive discussion of Shibley and other related cases, see Graham, supra note 43, at 1413-17.
262. 341 N.E.2d at 337. Plaintiffs also sought damages and costs. Id.
263. Id. at 339-40.
264. Id. at 339 (quoting Housh, 133 N.E.2d at 341).
265. Id. Plaintiffs alleged that buyers of the lists drew inferences about the ‘financial position, social habits, and general personality of the persons on the lists by virtue of the fact that they subscribe to certain publications and that this information is then used in determining the type of advertisement to be sent.‘ Id.
266. Id. It is worth noting that the plaintiffs seemed to erroneously place the thrust of their complaint on the fact that they received unwanted solicitations, rather than on the sale of the information by the magazine to the advertiser in the first place. As one commentator has noted, ‘Plaintiff obfuscated the privacy question by complaining that the sale of personality profiles subjected magazine subscribers to solicitations from direct mail advertisers.‘ Graham, supra note 157, at 1413.
267. Shibley, 341 N.E.2d at 339. The court stated ‘[i]t is clear from a reading of the authorities dealing with invasion of privacy that the ‘appropriation or exploitation of one's personality’ referred to ... those situations where the plaintiff's name or likeness is displayed to the public to indicate that the plaintiff indorses the defendant's product or business. ‘ Id. (citing W. Prosser, Law of Torts s 117 (4th ed. 1971)). The court then summarily dismissed the argument by stating that ‘[t]he activity complained of here does not fall within that classification.‘ Id.
268. See McCarthy, supra note 155, s 6.1; Reidenberg, Fortress or Frontier, supra note 63, at 226-27.
269. Shibley, 341 N.E.2d at 339-40.
270. Id. at 339 (referring to Ohio Rev. Code Ann. s 4503.26 (Anderson 1993)).
271. 269 F. Supp. 880 (S.D.N.Y.), aff'd, 386 F.2d 449 (2d Cir. 1967), cert. denied, 391 U.S. 915 (1968).
272. Id. at 884. In Lamont, the plaintiff claimed that subjecting motor vehicle registrants to the kind of solicitation that would flow from sale of registration lists was a ‘violation of the right to privacy and constitute [[[d] deprivation of ... liberty and property under the First, Fourth, Fifth, Ninth and Fourteenth Amendments to the United States Constitution.‘ Id. at 882. The Lamont court found that there was no ‘captive quality‘ in the solicitation. Id. at 883.
273. Id.
274. See supra notes 142-47 and accompanying text.
275. See Reidenberg, supra note 63, at 226; Graham, supra note 43, at 1417; Shorr, supra note 44, at 1831 & n.369.
276. As to Shibley's logic, Professor Reidenberg points out: ‘[i]n general, courts do not require an expectation of privacy or publicity as elements of this invasion of privacy. The Shibley court did not, in fact, assess whether the mailing list reflected Shibley's personality.‘ Reidenberg, Fortress or Frontier, supra note 63, at 226-27.
277. See supra note 163 and accompanying text, recounting deference to legislature exercised by Shibley court.
278. 652 N.E.2d 1351 (Ill. App. Ct. 1995).
279. Id. at 1356. Plaintiffs' claim grew out of a May 1992 settlement between American Express and the New York State Attorney General's Office whereby American Express agreed to disclose to all cardmembers the fact that it compiled information from cardmember card usage and sold that information to marketers and merchants. It further agreed to give cardmembers the opportunity to ‘opt out‘ of having

their names included on these lists. Peter Pae, American Express Co. Discloses It Gives Merchants Data on Cardholders' Habits, Wall St. J., May 14, 1992, at A3.
According to news articles released at the time of the settlement, American Express categorized and ranked cardmembers into six tiers based on spending habits (e.g., ‘Rodeo Drive Chic‘ or ‘Value Oriented‘). Id. To achieve this categorization, American Express analyzed ‘where [cardmembers] shop and how much they spend, and also consider[ed] behavioral characteristics and spending histories.‘ Dwyer, 652 N.E.2d at 1353.
American Express also created lists to target cardmembers who purchase specific types of items, and cardmembers who fell into various categories of shoppers, including ‘mail-order apparel buyers, home-improvement shoppers, electronics shoppers, luxury lodgers, card members with children, skiers, frequent business travelers, resort users, Asian/European travelers, luxury European car owners, or recent movers.‘ Id.
280. Id. at 1357.
281. 662 N.E.2d 423 (Ill. 1996).
282. The elements of intrusion upon seclusion under Illinois law are: 1) unauthorized intrusion or prying into defendant's seclusion; 2) intrusion which is objectionable to a reasonable man; 3) intrusion into a private matter; and 4) causation of anguish and suffering. Id. at 1354 (citing Melvin v. Buling, 490 N.E.2d 1011, 1013-14 (Ill. App. Ct. 1986)).
The court held that plaintiffs failed to establish the first element, ‘unauthorized intrusion,‘ reasoning that when the cardmembers use the card, they are ‘voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences.‘ Id.
283. The court dismissed this claim because the Illinois Consumer Fraud Act only provided private causes of action to ‘[a]ny person who suffers damage as a result of a violation of th[e] Act.‘ Id. at 1357 (quoting 815 Ill. Comp. Stat. 505/10a(a) (West 1992)). Because plaintiffs did not, and could not, allege damage from disclosure of this sort of information, their claim under the act was dismissed as well. Id.
284. The elements of tortious appropriation under Illinois law are: 1) appropriation, 2) without consent, 3) of one's name or likeness, 4) for another's use or benefit. Id. at 1355. This definition is fairly consistent with that of the Restatement and the majority of jurisdictions. See Restatement (Second) of Torts s 652(C) (1977); McCarthy, supra note 155, ss 6.1-.15.
285. Id. (citing Restatement (Second) of Torts s 652(C) cmt. a (1977)).
286. Id. at 1356.
287. Id. (citing Zacchini v. Scripps-Howard Broad. Co., 351 N.E.2d 454 (Ohio 1976), rev'd on other grounds, 433 U.S. 562 (1977)); Douglass v. Hustler Magazine, 769 F.2d 1128, 1138 (7th Cir. 1985); Annerino v. Dell Publ'g Co., 149 N.E.2d 761 (Ill. App. Ct. 1957); Eick v. Perk Dog Food Co., 106 N.E.2d 742 (Ill. App. Ct. 1952).
288. After reciting the parties' arguments, the court simply stated: ‘Even more persuasive is Shibley v. Time ....‘ Id. It provided neither an explanation of Shibley's reasoning nor any independent reasoning to dismiss the appropriation claim.
289. Id.
290. Id.
…

Balancing Consumer Privacy with Behavioral Targeting

Dustin D. Berger
Santa Clara Computer & High Tech. L.J.
Volume 7
Starting Page: 3
2011

[*17]…B. The Risks of Behavioral Targeting

Consumer and privacy advocates are concerned that the compilation of extensive profiles containing information about consumers and their behavior can harm consumers. This subsection explains how behavioral targeting can harm consumers and the circumstances when these harms can occur. It also explains how consumers are in a poor position to effectively manage the risks associated with profiling. Finally, it discusses profilers' attempts to manage these risks through anonymization.

1. How Behavioral Targeting Harms Consumers

Behavioral targeting is not a new phenomenon, nor does it occur solely on the Internet. Indeed, in 1999, the FTC became interested in ***18** the risks associated with behavioral targeting when DoubleClick, a company specializing in Internet-based behavioral advertising, purchased Abacus Direct, a direct marketing services corporation maintaining information on American customers' "offline" retail habits.[97] The FTC worried that DoubleClick would be able to combine its Internet consumer database with the purchased Abacus database describing consumer's "offline" habits[98] and that the combination would sharply increase the detail with which the merged organization would be able to view the consumers it had profiled.[99]

After investigating, the FTC concluded that its fears were unfounded because DoubleClick had not combined its Internet-based database with Abacus' "offline" database.[100] Nevertheless, the proliferation of behavioral targeting makes it likely that Internet profiling will become so much more extensive and thorough that Internet profiles will grow to contain as much detail as a combined DoubleClick database would have, even though the Internet profile is never merged with a source of "offline" information.

Nevertheless, as this part shows, the existence of these consumer profiles, replete with information about the consumer and his or her habits, puts all consumers in danger of (1) losing the ability to shield intimate and personal details of their private lives from the view of profilers who wish to use this data as a marketing tool, (2) embarrassment from the unexpected disclosure of details about a consumer that a consumer expected to remain private, (3) identity theft or other forms of financial fraud made possible by the richness of detailed information present in a consumer's profile, and even (4) the unexpected use of a consumer's profile to make adverse decisions about how to treat her.

First, consumer and privacy advocates criticize behavioral targeting because it results in the compilation of a sizable array of potentially sensitive data about the consumer that exists outside her ability to protect, control, or monitor.[101] Indeed, profiling arguably ***19** harms consumers regardless of how it is used because it results in an unprecedented loss of privacy. By merely participating in the Internet economy, consumers lose control over which details about their private lives are known,[102] and they have little control over who gets to learn of these details after the data passes into a profiler's hands.[103] Nor do consumers have any control over the way a profiler mines compiled data to construct a "picture" of an individual consumer, even though this data mining can generate a far more intrusive "picture" of the consumer's life than he might expect.[104] In creating this picture, the profiler learns and potentially communicates something private about the consumer that he has not authorized the profiler to know.[105]

Secondly, sometimes this unauthorized picture can be embarrassing, regardless of whether it is disclosed inadvertently or intentionally.[106] This embarrassment is itself a type of harm that the law has been willing to remedy in other contexts.[107]

Even worse, in the wrong hands, a consumer's profile could facilitate financial fraud or identity theft.[108] Thus, a consumer whose ***20** data is inappropriately disclosed might experience harm because she must take steps to prevent, monitor, or remedy identity theft or other financial fraud.[109]

Finally, consumer and privacy advocates also fear that the use of behavioral profiles to make decisions that may be inappropriate (or at least surprising) uses of consumer data.[110] For instance, insurers or potential creditors might wish to use a consumer's profile in an attempt to establish pricing for their products.[111] In addition, Internet retailers may use consumer data to engage in a practice of differential pricing for consumers based on a behavioral profile.[112]

2. The Mechanisms of Inappropriate Disclosure

When a profile paints an intrusive picture of a consumer, the collection of the profile itself may harm the consumer regardless of how the profile is used. But some other harms that consumer and privacy advocates anticipate are contingent on the inappropriate use ***21** or disclosure of consumer data. Understanding how inappropriate use or disclosure occurs, therefore, is a predicate to discussing the appropriate legislative or regulatory methods of preventing these harms.

First, ample anecdotal evidence shows that corporations and other consumer information profilers have difficulty securing their data.[113] There are a variety of overlapping threats. Corporations occasionally lose and misplace backup tapes[114] and other archival media.[115] They lose data when laptops (and, increasingly, also mobile devices like Blackberries[116]) containing sensitive data are lost or stolen.[117] Corporations occasionally lose data because hackers or malware penetrate their electronic defenses.[118] Sometimes they lose ***22** data to disgruntled employees.[119] Other times, data is lost because of bugs in Internet-enabled software.[120] This loss happens in spite of laws requiring these profilers to undergo expensive notification campaigns when they have such disclosure.[121] Some of these breaches might be a result of a profiler's negligent safeguards, but, in other cases, profilers are victims of others' malfeasance in spite of

instituting safeguards. Moreover, everyone must wonder how many data losses go undetected and unreported.[122]

In addition to losing data describing their customers, profilers often share the data they collect about consumers. Companies commonly share a customer's information across their business units, and, of course, with contractors the company employs to provide its products or services.[123] Some companies sell valuable data to ***23** "partners" that use the data for marketing purposes not connected to the original company's business units.[124]

Profilers may also be required to share the data they collect with law enforcement authorities and litigants.[125] Indeed, a person's right to privacy relative to government agents in this context is much weaker than consumers probably expect.[126] An individual's right to privacy in any information that a third party holds is extremely limited.[127] Many profilers include warnings in their privacy statements that a consumer's profile may have to be disclosed to law enforcement authorities.[128] And, this data may occasionally be at risk because it could be discoverable in civil litigation.[129]

3. The Role of the Consumer

Consumers are in poor positions to protect themselves from these harms. They lack the information that they need to make rational decisions about whether to participate in activities on the Internet that involve behavioral targeting.

The fundamental calculus of risk aversion is a familiar tort ***24** concept to most lawyers. As Judge Learned Hand wrote:

The degree of care demanded of a person by an occasion is the resultant of three factors: the likelihood that his conduct will injure others, taken with the seriousness of the injury if it happens, and balanced against the interest which he must sacrifice to avoid the risk.[130]

Judge Hand later expressed this analysis in a formula:

[I]f the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e. whether $B < PL$.[131]

In short, under Judge Hand's intuitive analysis, a person is negligent in taking precautions to avoid a particular harm when the person refuses to incur a precautionary cost or burden that is less than the magnitude of the loss multiplied by the probability of the loss.[132]

Judge Hand's calculation is readily adaptable to the analysis that consumers must perform in deciding whether to assume the risks inherent in taking part in an activity on the Internet involving behavioral targeting. Under Judge Hand's formula, a consumer should be willing to participate in an activity involving behavioral targeting as long as the value the consumer gets from participation exceeds the risk of loss. The risk of loss, just as in the classic tort law analysis, is equal to the probability of loss multiplied by the expected magnitude of the loss.

Consumers are not able to readily determine the risk of loss inherent in participating in activities involving behavioral targeting because they lack accurate information about the probability of the loss and the magnitude of the harm that could occur. Thus, consumers are in a poor position to decide when and how to protect themselves from the harms inherent in behavioral targeting. Indeed, as the foregoing examples have shown, consumers cannot assess the potential magnitude of harm because they likely do not know when profilers are collecting and using their data. Consumers also lack information about what data the profilers collect or guess about them. In addition, consumers are unable to assess the probability of harm occurring because they do not know how profilers use their behavioral profile or the prevalence of inappropriate use or ***25** disclosure.[133]

The consumer's inability to accurately assess the magnitude of loss begins with her inadequate understanding of how much data the profilers can obtain and how the data describes even some of the most intimate details about the consumer.[134] Consumer and privacy advocates analogize the non-consensual use of an Internet user's information to a wiretap of a telephone call.[135] They suggest that consumers would rightly be upset if someone listened to their phone conversations without consent, regardless of the purpose of the eavesdropping or the steps used to safeguard the record of the information learned from the eavesdropping.[136] Consumers do not expect their phone calls to be intercepted nor for revealed personal details to be cataloged.[137]

Likewise, consumers do not expect their ISPs to listen in on their web-based “conversations.” On the contrary, consumers expect their ISPs to serve merely as a conduit for their information.[138] Similarly, when a consumer visits a website, he expects to receive information and may not expect to be tracked and profiled. Consumer advocates fear that as Internet users begin to understand the extent of the profiling that online marketers perform, they will begin to avoid using the Internet in spite of its efficiency and convenience.[139]

These breaches of consumer expectation may be especially worrisome when profilers collect sensitive elements of personal information that have a heightened potential for abuse. For instance, the FTC notes that financial and health information are especially sensitive.[140] Financial details are rife with the potential for financial fraud.[141] Health information could easily become an embarrassment, ***26** an unwelcome intrusion on a consumer's privacy, and might, in an extreme case, even hamper the consumer's ability to get employment or insurance.[142] Privacy advocates are also understandably concerned about the profiling of children, because they may not understand the privacy concerns as an adult might, nor are they capable of legally assenting to a service provider's privacy policy or terms of use.[143] A consumer's physical location is also sensitive because of its significance in allowing the consumer to be personally identified.[144]

Consumers are also likely to be surprised that profilers use mathematical models to “guess” the characteristics of a consumer.[145] Statistical techniques make it possible that a consumer's profile might not only include factual information about a consumer's Internet use, but also inferred information, which may or may not be correct.[146] Because profilers potentially have access to information about the habits, likes, and propensities of many consumers, they may “guess” or “predict” unknown information about consumers through a statistical process of comparing them to other consumers with known information.[147] In a sense, this process is exactly what Amazon or Netflix does when generating suggestions for books, movies, or other items: they suggest to

consumers other items that similar consumers (meaning, in this sense, consumers with similar preferences or purchases) liked. But, now, instead of guessing a consumer's preference for a good or service, the profiler guesses information about the consumer.[148]

***27** Because consumers lack marketers' sophisticated understanding of the models that can be used to predict a consumer's demographic information, their intuitive assessment of the magnitude of the harm of participating in an Internet activity involving behavioral targeting is likely to be too low. If inferred demographic characteristics are stored along with other elements in a consumer's profile as factual information, and then inappropriately disclosed, even inadvertently, it could make the magnitude of embarrassment even worse. Even when the inferred information is accurate, it allows profilers to create an even more comprehensive profile of a consumer that contains information the consumer did not even know he or she was disclosing.[149]

For instance, researchers at the Massachusetts Institute of Technology, after analyzing over 4,000 students' Facebook profiles, were recently "able to predict, with 78 percent accuracy, whether a profile belonged to a gay male."[150] The inference about a person's sexuality, if it is unexpectedly or inappropriately disclosed, could be deeply intrusive, embarrassing, and harmful for consumers, regardless of whether the inference is correct.

Thus, because consumers lack information about what information profilers collect (or guess) and how sensitive the information is, consumers are likely to underestimate the magnitude of harm that can occur because of their participation in activities that involve behavioral targeting. However, consumers have even less information to aid them in understanding the likelihood that harm will occur.

For instance, in May 2010, Facebook "users discovered a glitch that gave them access to supposedly private information in the accounts of their Facebook friends, like chat conversations."[151] This presents consumers with the difficult question of trying to assess the likelihood that a company like Facebook will disclose their personal data in a way that can harm them. As an industry analyst noted, "[Facebook users] have to ask whether it is a platform worthy of their trust."[152] And a recent complaint against Facebook in the FTC even charged that Facebook also intentionally "manipulate[s] the privacy settings of users and its own privacy policy so that it can take ***28** personal information provided by users for a limited purpose and make it widely available for commercial purposes."[153] Facebook users are especially indignant about the inadvertent disclosure because "most people signed up for Facebook with the understanding that their information would be available only to an approved circle of friends."[154]

The Facebook example is simply an unusually public example of an inadvertent data breach. As part I.B.2 described, there is ample anecdotal evidence showing that data breaches happen continually under a variety of circumstances. The typical consumer simply has no way of intelligently assessing the thoroughness of the precautions that a profiler takes to protect the consumer's data. Consequently, the consumer simply cannot assess the probability that a profiler's use of behavioral targeting will harm them.

4. Mitigation Through Anonymization

Profilers have attempted to mitigate some risks of harm to consumers through anonymization.[155] Anonymization is an effort to take a set of data, such as a database containing consumer profiles, and eliminate those characteristics of the set that would allow someone to discern the identities of the consumers described in the dataset.[156] Behavioral advertisers, during public hearings and proceedings before the FTC, expressed their belief that information that does not identify a consumer's identity poses no significant risk to the consumer's privacy.[157] Other behavioral advertisers have touted their efforts to anonymize their data by severing the direct ties between a consumer's profile and the consumer's identity.[158] Indeed, behavioral advertisers often have little need to know the identity of a consumer to effectively profile and advertise to that consumer.[159] Of ***29** course, anonymization would mean, at a minimum, the elimination of obviously identifying information, like a consumer's name, address, social security number, e-mail address, phone number, and so forth.[160]

But computer scientists caution that even in datasets where this obviously identifying information has been removed, it is remarkably easy to identify particular users.[161] Researchers were able to identify the users associated with anonymized information from the Netflix Prize dataset using data gleaned from IMDB (a movie-related website that offers users the opportunity to rate movies).[162] Netflix offered the Prize to any researcher who could improve Netflix's movie suggestion technique by a designated margin, and could demonstrate that improvement on a sample “anonymous” dataset of consumers' movie ratings that Netflix made available.[163] The researchers found that if they disregarded an anonymous consumer's favorable ratings of the 100 most popular movies from the Netflix data, the pattern of consumer likes and dislikes was fairly unique.[164] Then, through correlation of this pattern of unique likes and dislikes (between the Netflix and IMDB data), the researchers were able to discern the consumers' identities.[165] And, although Netflix's anonymization efforts may have been incomplete, the scientists suggest that their methods for reconstructing consumers' identities from anonymized data would have worked even if Netflix had modified dates, added deliberate errors, or taken other steps to obfuscate the consumers' identities whose preferences the data described.[166] Netflix cancelled plans for a second Netflix Prize because of the attendant privacy concerns.[167]

Other researchers have come to similar conclusions. Stanford University researchers have reported that a date of birth is highly ***30** valuable when attempting to discern someone's identity.[168] Other researchers have concluded that about half of the U.S. population can be identified using only their gender, date of birth, and the city of residence.[169] In essence, even information that does not appear to disclose a person's identity can readily do so when combined with other data.[170]

Indeed, the AOL dataset that led to the New York Times reporters' identification of Ms. Arnold was anonymized before AOL released it for scholarly study.[171] AOL later apologized and removed the data, which they claimed had not been duly authorized for release.[172] Because of the release, AOL's chief technology officer resigned and AOL fired a whole team of researchers.[173]

C. The Benefits of Behavioral Targeting

While the privacy concerns associated with behavioral targeting are significant, the benefits of this technology are compelling and far less contingent than the risks. Behavioral advertising, for instance, is one way of funding the generation and delivery of content on the Internet.[174] Other forms of behavioral targeting promise to connect consumers with old friends, new friends, and useful products the consumer will likely enjoy. Internet businesses are already using behavioral targeting to provide these benefits to consumers. On the other hand, the risks associated with behavioral targeting are largely contingent on some kind of unexpected or improper behavior, such as an inappropriate disclosure or misuse of consumer profile data. Thus, if the risks of harm to consumers can be effectively managed, and service providers share the benefits of the technology with their customers, the technology benefits both profilers and consumers.

Behavioral advertising, for instance, allows content providers to fund the delivery of web-based content and services to consumers on the Internet.[175] One way of providing web-based content is to require ***31** consumers to pay directly for the service (a "subscription-based" approach).[176] Another is to follow the broadcast television model of allowing advertising to pay content providers for providing a service to consumers (an "advertising-based" model).[177]

The advertising-based approach is advantageous for both advertisers and consumers. Behavioral advertising, as compared to other forms of advertising, offers advertisers an efficient method of precisely targeting a valuable demographic.[178] It is, in fact, so efficient that it offers companies "the highest return on investment for dollars spent on e-advertising-a value that is only diminished by the controversial nature of [the] tracking technology."[179] Consumers respond to this new technology. They are "at least ten percent more receptive to behaviorally targeted advertisements than to contextually targeted advertisements."[180] The market for behavioral advertising is expected to grow "from $350 million in 2006 to $3.8 billion by 2011."[181] The technology also helps small businesses compete, even when their customers would ordinarily be too diffuse to reach through other advertising outlets.[182]

Indeed, Microsoft's CEO, Steve Ballmer lauded the technology: "The more we know about customer behavior, the more every ad is relevant."[183] This relevance works both ways. Of course, this relevance means that the advertiser is able to use its advertising budget to target those customers it most wishes to reach. But it also means that when a consumer sees an ad, it is more likely to be ***32** relevant (and therefore useful[184]) to him or her.[185] Consumers will see ads that are more likely to be appealing, useful, and appropriately tailored to their sensibilities.[186] Revenue resulting from the ad's placement then can fund Internet-based content and services.[187] Google credits revenue from online advertising for funding its free e-mail, search, and geographic information services.[188]

Consumers already reap the benefits of free services funded through behavioral advertising.[189] In spite of the potential for profiling to harm consumers, the prevalence of harm stemming from profiling appears quite low.[190] This is not to say that abuse and misuse do not occur. But, considering the concrete and widespread benefits that behavioral targeting already provides, it makes little sense to enact a remedial scheme that hampers the advancement of a generally helpful technology.[191] Indeed, behavioral advertising is already being used to aggregate a commodity-consumer information-that, to the individual consumer, has little exchange value into a valuable product that allows the consumer to access relevant and free Internet content.[192]

And, the benefits of behavioral targeting are not limited to the behavioral advertising context. Other forms of behavioral targeting also provide benefits for consumers. Facebook uses consumers' profiles to connect its customers to other potential acquaintances. Amazon suggests products that consumers might enjoy.[193] Netflix suggests movies the consumer might enjoy. Not only are these ***33** benefits compelling, but they come without some of the dangers associated with behavioral advertising. For instance, consumers often volunteer the information the companies use to make these recommendations.[194] Often, a consumer can see why a website offered a particular recommendation.[195] Of course, even this form of profiling is not without privacy risks. In fact, the risks may be greater; companies like Amazon and Facebook store personally identifying information about consumers (name, address, phone number, and e-mail), so the risks of identity theft and embarrassment are heightened with respect to the unexpected disclosure of this data.

The benefits of behavioral targeting are, in fact, so compelling that some Internet service providers have attempted to appropriate for themselves the financial benefits of behavioral advertising. A recently filed complaint in California alleges that several Internet service providers (ISPs) are using the deep packet inspection form of behavioral advertising to turn their clients' data into a revenue stream for themselves, even though the ISP's clients are already directly paying for service.[196] These ISPs are using a device from NebuAd[197] that plugs directly into the ISP's network equipment, allowing the equipment access to all Internet data sent to and from any and all of the ISP's customers.[198] The complaint also alleges that adequate notice was not given to the customers whose Internet traffic was rigorously deconstructed, examined, analyzed, and manipulated.[199] The complaint further alleges that following an opt-out procedure did not actually opt the consumer out of this process of constant inspection of his or her Internet traffic.[200] Similar allegations are levied, in the United Kingdom, against British Telecom and Phorm, another seller of deep packet inspection appliances.[201] British ***34** Telecom admits that it did not obtain consumers' consent to employ these appliances.[202]
…

Footnotes

97. DoubleClick, 154 F. Supp. 2d at 505.
98. Id.
99. See id. (noting that the combination could "create a super-database capable of matching [consumers'] online activities with their names and addresses"); see also Complaint and Request for Injunction, Request for Investigation and for Other Relief at 6-10, In the Matter of DoubleClick, before the Fed. Trade Comm'n (Feb. 10, 2000), available at http://www.epic.org/privacy/internet/ftc/DCLK_complaint.pdf (noting that a combined database would violate consumers' expectations of privacy and alleging that it constitutes an unfair practice under the FTC Act).
100. In re DoubleClick, 154 F. Supp. 2d at 506.
101. Cf. Robert Sprague & Corey Ciocchetti, Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws, 19 Alb. L.J. Sci. & Tech. 91, 93 (2009) (discussing how consumers lose control over personally identifying information (PII) when they disclose it to businesses, and how businesses use PII for data mining).
102. Id. at 93; see also id. at 111 (discussing the embarrassment inherent in a physician permitting an "unmarried man with no medical training to be present when a woman gave birth").
103. Id. at 93.

104. Id. at 95-96.
105. See id. Some behavior advertisers do not believe that consumers should have a right of privacy in these details. PRINCIPLES, supra note 7, at 31 (“These commenters suggested that consumers do not own the data that websites collect about them, and that there is no precedent for giving consumers the ability to dictate the terms upon which they use a website.”). See also Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 199 (1890), available at http:// groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_ warr2.html (“[T]he individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent.”) (emphasis added).
106. See Barbaro & Zeller, supra note 1.
107. Warren & Brandeis, supra note 105, at 197. (“[M]odern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.”). Warren and Brandeis, however, premised their influential ideas about privacy on the problem of gossipy newspapers. John L. Diamond, et. al, Understanding Torts 387, n.2 (3rd. ed. 2007). Because the social value of gossip is low, it was comparatively easy for courts to follow the Warren and Brandeis article into recognizing a right to privacy. However, with behavioral targeting's comparatively substantial benefits to consumers and society, it is more difficult to make a plausible case that consumers have an absolute right to privacy or complete control of their data. See infra part II.C.
108. See Sprague & Ciocchetti, supra note 101, at 101-02 (describing the risks of identity theft and financial fraud inherent with the disclosure of personally identifying information (PII)). While the profiles that result from behavioral targeting may not contain PII, the aggregation of even non-personally identifying information ultimately forms such a complete picture of a consumer as to pose the same risks. See Barbaro & Zeller, supra note 1.
109. E.g., Sandy Kleffman, Kaiser Warns Nearly 30,000 Employees of Data Breach, San Jose Mercury News, Feb. 6, 2009, http://www.mercurynews.com/ci_ 11646163?nclick_check=1 (last visited Apr. 19, 2009) (describing how a Kaiser Permanente data breach is believed to have resulted in identity theft for several Kaiser Permanente employees whose data was described in the data lost in the breach). See also Federal Trade Commission, Defend: Recover From Identity Theft, Fighting Back Against Identity Theft, http:// www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html (last visited Apr. 19, 2009) (describing the many steps an identity theft must go through to minimize the effects of the crime). But see Sasha Romanosky, et al., Do Data Breach Disclosure Laws Reduce Identity Theft?, Seventh Workshop on the Economics of Information Security, June 25-28, 2008, http:// weis2008.econinfosec.org/papers/Romanosky.pdf (“The probability of becoming a victim to identity theft as a result of a data breach is very low, around only 2%.”). Even if true, this observation confirms that there is a measurable positive correlation between identity theft and data breach. Nevertheless, it can be difficult to confirm whether incidents of identity theft are attributable to a particular data breach. See Randy Ludlow & Holly Zacariah, Hacked Off: Data Thefts Leave Ohio University Scrambling, Students and Alumni Steaming, Columbus Dispatch, Jun. 19, 2006, at 1A (noting that although officials were not aware of any confirmed cases of identity theft related to a data breach, 24 cases of identity theft were under investigation).
110. Center for Democracy and Technology, Privacy Impact, Guide to Behavioral Advertising, Oct. 27, 2009, http://www.cdt.org/content/privacy-impact (last visited Mar. 28, 2010) [hereinafter Privacy Impact].
111. Id. (“Behavioral profiles, particularly those that can be tied to an identifiable individual, may also be a tempting source of information for companies making decisions about people's credit, insurance or employment.”).
112. Id.
113. See generally Sprague & Ciocchetti, supra note 101, at 97-101.
114. E.g., Jon Oltsik, Perspective: One Less Data Breach Method to Fret About, CNet News, Feb. 7, 2006, http://news.cnet.com/One-less-data-breach-method-to-fret-about/2010-1029_3-6035850.html (last visited April 13, 2009) (describing data breaches at Bank of America, Citibank, Marriott, and Time

Warner); Ingrid Marson, Marriott Loses Data on 200,000 Customers, CNet News, Jan. 3, 2006, http://news.cnet.com/Marriott-loses-data-on-200,000-customers/2100-1029_3-6015768.html (describing data breach at Marriott); Dawn Kawamoto, Data for 600,000 Time Warner Employees MIA, CNet News, May 2, 2005, http://news.cnet.com/Data-for-600,000-Time-Warner-employees-MIA/2100-1029_3-5692534.html (describing loss of Time Warner backup tapes during transport to storage facility).
115. E.g., Leo King, Virgin Media Loses Unencrypted CD With 3,000 Customer Bank Details, Computerworld UK, June 23, 2008, http:// www.computerworlduk.com/management/security/data-control/news/index.cfm? newsid=9687 (describing how Virgin Media lost a CD containing unencrypted customer banking details in spite of a company policy prohibiting this data from being transmitted without encryption).
116. E.g., Cabinet Data on Stolen BlackBerry, BBC News, Apr. 11, 2009, http://news.bbc.co.uk/1/hi/uk/7994850.stm (last visited Apr. 13, 2009), available at http://news.bbc.co.uk/2/hi/uk_news/7994850.stm; Yuki Noguchi, Lost a BlackBerry? Data Could Open A Security Breach, Wash. Post, Jul. 25, 2005, at A01, available at http://www.washingtonpost.com/wp-dyn/content/article/2005/07/24/AR2005072401135.html.
117. E.g., Robert McMillan, Boeing Laptop Theft Puts U.S. Data Breach Tally Over 100M; A Privacy Group Has Kept Tabs on Incidents Since February 2005, Computerworld, Dec. 15, 2006, http:// www.computerworld.com/action/article.do? command=viewArticleBasic&articleId=9006140 (discussing data breaches associated with lost laptops at Boeing); Nathan McFeters, Stanford University Data Breach Leaks Sensitive Information of Approximately 62,000 Employees, Zero Day, June 23, 2008, http://blogs.zdnet.com/security/?p=1326.
118. E.g., Joel Hruska, Malware Infestation Responsible for Credit Card Data Breach, Ars Technica, Jan. 20, 2009, http:// arstechnica.com/security/news/2009/01/malware-infestation-responsible-for-credit-card-data-breach.ars (describing a credit card data breach at a major processing company stemming from a malware infection and indicating the company does not plan to provide credit monitoring to affected persons because the company concluded the data breach did not pose this risk to consumers); Kim Zetter, Card Processor Admits to Large Data Breach, Wired.com, Jan. 20, 2009, http://blog.wired.com/27bstroke6/2009/01/card-processor.html (describing the same data breach as the result of hacking); Brian Krebs, Justice Breyer Is Among Victims in Data Breach Caused by File Sharing, Wash. Post, July 9, 2008, at A01 (describing data breaches resulting from employee use of peer-to-peer file sharing programs). The distinction between malware and hacking is, perhaps, misleading. Hackers often use malware as the instrumentality of their fraud. See Zetter, supra note 118. Data breaches are not unique to corporations. “Higher education is a juicy target [for hackers] because it compiles so much personal information in so many places.” Ludlow and Zacariah, supra note 109.
119. E.g., Brian Krebs, Data Breaches Up Almost 50 Percent, Affecting Records of 35.7 Million People, Wash. Post, Jan. 6, 2009, at D02 (noting “the percentage of breaches attributed to data theft from current and former employees more than doubled from 7 percent in 2007 to nearly 16 percent in 2008.”).
120. Jason Kincaid, Google Privacy Blunder Shares Your Docs Without Permission, TechCrunch, Mar. 7, 2009, http:// www.techcrunch.com/2009/03/07/huge-google-privacy-blunder-shares-your-docs-without-permission/ (describing a problem in Google Docs that inadvertently allowed former collaborators to access documents the owner had revoked access to); Jenna Wortham, Facebook Glitch Brings New Privacy Worries, N.Y. Times, May 6, 2010, at B1. This sort of problem can be expected to become even more common as rapidly developed software becomes more common. This software development approach speeds the release of new features to users, but at the “cost” of rigorous testing. Or, perhaps a better way to put it is that the earliest users perform the testing that software testers might have done.
121. E.g., Brian Krebs, Data Breaches Are More Costly Than Ever, Wash. Post, Feb. 3, 2009, at D03 (according to a new study, “[o]rganizations that experienced a data breach in 2008 paid an average of $6.6 million last year to rebuild their brand image and retain customers ....”); Cal. Civ. Code §§ 1798.29, 1798.82, and 1798.84 (West 2008); Colo. Rev. Stat. § 6-1-716 (2008); Sprague & Ciocchetti, supra note 101, at 101-02. Note that, while data breach laws are common, most do not require the breached entity to do anything more than notify consumers of the breach. Id. at 102.

122. See, e.g., Thomas Claburn, Most Security Breaches Go Unreported, Information Week, Aug. 1, 2008, http:// www.informationweek.com/news/security/attacks/showArticle.jhtml? articleID=209901208 (noting that according to one survey, "[m]ore than 89% of security incidents went unreported in 2007.").
123. Daniel Solove et al., Information Privacy Law 623 (2d ed. 2006); Corey A. Ciocchetti, The Future of Privacy Policies: A Privacy Nutrition Label Filled With Fair Information Practices, 26 J. Marshall J. Computer & Info. L. 1, 29-30 (2008).
124. Solove, supra note 123, at 623; Ciocchetti, supra note 123, at 18.
125. See infra notes 128-131.
126. See United States v. Miller, 425 U.S. 435, 442-44 (1976) (concluding a person has no reasonable expectation of privacy in his bank's imaged check records, even though that consumer gives data to the bank for a limited purpose, because when a person gives information to a third party, the person takes the risk that the third party will disclose the data to the government); California v. Greenwood, 486 U.S. 35, 40-41 (1988) (concluding a person has no expectation of privacy in trash placed for collection outside the home, even though it may reveal intimate details of the private behavior going on inside the house, because when left in public, the trash is accessible to animals, children, and others). When a person has no reasonable expectation of privacy in a certain piece of information, the legal result is that government agents need neither a warrant nor probable cause to obtain the information. See Smith v. Maryland, 442 U.S. 735, 740 (1979) (confirming that Fourth Amendment protections can attach only when a person has a reasonable expectation of privacy). See generally Sprague & Ciocchetti, supra note 101, at 114-16.
127. Sprague & Ciocchetti, supra note 101, at 116 (surveying cases and concluding that individuals have no right to privacy in the "'to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account"' or "'subscriber information provided to an internet provider"'); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008).
128. E.g., Facebook, Privacy Policy, http://www.facebook.com/policy.php? ref=pf (last visited Apr. 19, 2009) ("We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law."); Netflix, Privacy Policy, http://www.netflix.com/PrivacyPolicy (last visited Apr. 19, 2009) ("Netflix also reserves the right to disclose personal information when we reasonably believe disclosure is required by law, if we reasonably believe disclosure is necessary to establish or exercise legal rights, or in situations involving potential threats to physical safety.").
129. Privacy Impact, supra note 110.
130. Conway v. O'Brien, 111 F.2d 611, 612 (2d Cir. 1940).
131. United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947).
132. See id.; See also John L. Diamond, et. al., Understanding Torts 69 (2d ed. 2000).
133. Privacy Impact, supra note 110. See also Letter from Alan Davidson, Senior Policy Counsel and Head of U.S. Public Policy, Google Inc. to Jessica Rich, Federal Trade Commission (Apr. 4, 2008), available at http:// www.ftc.gov/os/comments/behavioraladprinciples/080404google.pdf [hereinafter Google Letter] (explaining that Google is concerned with building trust with users through "transparency" in behavioral advertising, and, in particular, "being upfront with our users about what information we collect and how we use it").
134. Privacy Impact, supra note 110.
135. See Statement, supra note 62, at 16, 21-29.
136. See id. at 15-16.
137. See id.
138. See id. at 1.
139. Id. at 8.
140. PRINCIPLES, supra note 7, at 42; see also Chloe Albanesius, Should Online Ads Be Allowed to Know If You Have AIDS?, PC Magazine, Apr. 11, 2008, http://www.pcmag.com/article2/0,2817,2283076,00.asp.
141. See PRINCIPLES, supra note 7, at 42-44.
142. See Privacy Impact, supra note 110.

143. See id.; Jeffrey Ferriell & Michael Navin, Understanding Contracts, 509-10 (2004) (noting that, in contract law, children are not capable of "adequately protecting their own interests."). Congress was also concerned, and it expressed that concern when it passed the Children's Online Privacy Protection Act ("COPPA"). See 15 U.S.C. §§ 6501-06 (2000). COPPA defines a child as a person under 13, leaving children over the age of 13 without enhanced privacy protection. 15 U.S.C. § 6501 (2000).
144. Privacy Impact, supra note 110. The CDT's statement also indicates that the laws that protect health information within the health care sector might not apply outside this context. Id.
145. See Center for Digital Democracy et al., Online Behavioral Tracking and Targeting, Legislative Primer 3 (2009), http:// www.uspirg.org/uploads/s6/9h/s69h7ytWnmbOJE-V2uGd4w/Online-Privacy---Legislative-Primer.pdf [hereinafter Primer]; Report to Congress, supra note 31, at 5-6.
146. See Jian Hu et al., Demographic Prediction Based on User's Browsing Behavior 151 (2007), http://www2007.org/papers/paper686.pdf (last visited Feb. 10, 2011) (proposing a method for predicting basic demographic information of consumers on the internet).
147. See id. While it is not known how prevalent these inferential techniques are today, the existence of the research attests to the value of making guesses about key demographic characteristics of consumers that enable improved ad targeting.
148. Hu, supra note 146, at 1; Report to Congress, supra note 31, at 4-6.
149. See Primer, supra note 145, at 3.
150. Steve Lohr, How Privacy Vanishes Online, N.Y. Times, Mar. 17, 2010, at A1.
151. Jenna Wortham, Facebook Glitch Brings New Privacy Worries, N.Y. Times, May 6, 2010, at B1.
152. Id.
153. Id.
154. Id.
155. See, e.g., Google Letter, supra note 133, at 8; Complaint at 24, Valentine v. NebuAd, No. CV 08 5113 (N.D. Cal. Nov. 10, 2008), available at http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/.
156. Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, at 111-12, Proceedings of the 2008 IEEE Symposium on Security and Privacy (2008), available at http://userweb.cs.utexas.edu/~ shmat/shmat_oak08netflix.pdf, at 1-2.
157. Principles, supra note 7, at 20-21.
158. Google Letter, supra note 133, at 8 (noting Google's decision to anonymize IP addresses and cookie-based identification numbers after 18 months, even when these are not personally identifying, because "we believe that our users would prefer that we further anonymize this data after a reasonable period of time.").
159. DoubleClick, 154 F. Supp. 2d at 503-05 (describing how DoubleClick engages in behavioral advertising without knowing a user's identity).
160. See id.
161. Id.
162. Id.
163. Netflix, Netflix Prize, http://www.netflixprize.com (last visited May 12, 2009).
164. Bruce Schneier, Why 'Anonymous' Data Sometimes Isn't, Wired.com, Dec. 13, 2007, http:// www.wired.com/politics/security/commentary/securitymatters/2007/12/securitymatters_ 1213 (describing the Narayanan and Shmatikov work).
165. Id.
166. Id. When a reputable organization like Netflix fails to implement effective anonymization of a dataset that they intended to publicly release, it is easy to imagine other profilers making the same mistake in the maintenance of their own profiles, especially if they do not anticipate researchers and others testing the anonymization.
167. Lohr, supra note 150.
168. Schneier, supra note 164.
169. Id.

170. Id.
171. Id.
172. Id.
173. Schneier, supra note 164.
174. See infra notes 176-78.
175. Google Letter, supra note 133, at 2; Behavioral Advertising: Industry Practice and Consumers' Expectations Before the Joint Hearing of the Subcomm. on Communications, Technology and the Internet and the Subcomm. on Commerce, Trade and Consumer Protection of the H Comm. On Energy and Commerce Committee, 111th Cong. 3 (2009), available at http:// energycommerce.house.gov/Press_111/20090618/testimony_toth.pdf (Testimony of Anne Toth, Vice President of Policy and Head of Privacy, Yahoo! Inc.); Principles, supra note 7, at 1 ("[Consumers] may also benefit, however, from the free content that online advertising generally supports, as well as the personalization of advertising that many consumers appear to value.").
176. Hotaling, supra note 13, at 540.
177. Id.
178. Id. at 533-38.
179. Id. at 536.
180. Id. at 538 (quoting Tameka Kee, Revenue Science Finds Behavioral Targeting Ads 22% More Effective, MediaPost Publications, Sep. 12, 2007, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=67293). Contextually targeted advertisements are those that are targeted without the use of a consumer profile; Principles, supra note 7, at 29 ("[C]ontextual advertising differs from behaviorally targeted advertising because it is based only on the content of a particular website or search query, rather than on information about the consumer collected over time.").
181. Hotaling, supra note 13, at 539.
182. Google Letter, supra note 133, at 2. This efficiency is especially true when one thinks of the limited advertising budgets of small businesses-especially new small businesses.
183. Hotaling, supra note 13, at 536-37.
184. Google Letter, supra note 133, at 2.
185. See Principles, supra note 7, at 1, 6, 9-10.
186. Id.
187. Id.; Google Letter, supra note 133, at 2.
188. Google Letter, supra note 133, at 2.
189. Id.
190. See Bennet Kelley, Privacy and Online Behavioral Advertising, 11 J. of Internet Law 24, Dec. 2007 (noting that a "recurring theme" during the FTC's hearings was "the failure of those advocating further regulation to demonstrate any specific instances of harm."). One of the FTC's Commissioners, Mozelle Thompson, is reported as saying "the FTC should not take any action at all in the absence of evidence of consumer harm." Id. See also Diane Bartz, FTC Urged to Limit Behavioral Advertising, EWeek, Apr. 18, 2008 (reporting that the American Advertising Federation, Association of National Advertisers, and other organizations had issued a statement asserting that "any additional principles or guidelines should be issued only after the [FTC] specifically identifies harms and concerns so that business is in a position to consider and address them").
191. See Kelley, supra note 190; Bartz, supra note 190.
192. Consumer data may have little exchange value, but obviously has other value for consumers.
193. Amazon.com, Help, http:// www.amazon.com/gp/help/customer/display.html (last visited May 12, 2009).
194. E.g., id.
195. E.g., id.
196. Complaint at 23, Valentine v. NebuAd, No. CV 08 5113 (N.D. Cal. Nov. 10, 2008), available at http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/ (according

to Bob Dykes, NebuAd's CEO: “The ISPs have not been able share in ad revenue and wealth creation around the publishing side of the internet.”).
197. Id. at 16-17.
198. Id.; See generally supra Part I.A.
199. Complaint at 36, Valentine v. NebuAd, No. CV 08 5113 (N.D. Cal. Nov. 10, 2008), available at http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv05113/208758/1/.
200. Id. at 24-25. The opt-out procedure allegedly prevented the consumer from receiving targeted ads, but did nothing to stop the NebuAd appliances from performing deep packet inspection on all of the data the consumer sent to or received from devices on the internet. Id.
201. Kevin J. O'Brien, Use of Web Tracking Tool Raises Privacy Issue in Britain, N.Y. Times, Apr. 14, 2009.
202. Id.

The Search for a Viable Cause of Action Against Private Individuals Who Use Cookies to Obtain Personal Information

Jenna L. White
Syracuse Law Review
Volume: 55
Starting Page: 653
2005

Introduction

The use of cookies has garnered much attention in both the national media and the courtroom.[1] In fact, over the past few years, federal courts *654 have entertained several cases in which private individuals have challenged commercial organizations' use of cookies.[2] Some of these plaintiffs3 brought claims under Title I ("Wiretap Act")4 and Title II ("Stored Communications Act")5 of the Electronic Communications Privacy Act, and the Computer Fraud and Abuse Act ("CFAA").6. This Note uses these recent commercial cases as a framework to analyze a hypothetical plaintiff's potential success under these statutes after a private individual uses cookies to access the plaintiff's personal information. This Note submits that an individual whose personal information has been accessed by a private individual using cookies will be unable to obtain redress under the Stored Communications Act, the CFAA, or the Wiretap Act.

C. The Hypothetical

Victim had been receiving threatening e-mails and telephone calls for several months. The messages threatened Victim's life, and the lives of his wife and children. Victim desperately wanted to determine the stalker's identity so he could inform the police and they could make a speedy arrest. After serious thought, Victim compiled a list of possible suspects. One of the possible suspects was Target, a former business colleague with whom Victim had serious personal difficulties. To help with the identification, Victim hired a private detective, Smith, who suggested that he and Victim use cookies to determine the stalker's identity.

There are several ways Smith could use cookies to obtain this information. One of the available programs is SpyNet/PeepNet.[30] This program can "replay a web-browsing session."[31] Using this program, the person seeking to duplicate a web-browsing session will "sniff [cookies] *658 off the network."[32] Then, the program user will visit the website in question, supply his own login information, receive his own cookie, and substitute the "sniffed" "unique identifier" for his own.[33] The next time he logs on to this website, the SpyNet/PeepNet user can "masquerade" as the first user.[34]

For the purposes of this hypothetical, Smith used the following strategy to capture the information he needed. Smith replied to an e-mail Victim had received from the stalker, providing a link to a website housed on Smith's office server. Target received the e-mail and upon Target's first visit to Smith's web page, Smith's server placed a cookie on Target's system.[35] Even more specific than the "unique value of the cookie returned variable" was the information

gleaned when Target registered himself at Smith's website and this information was associated with the cookie.[36] When Target registered himself, he did so using POST submissions.[37] It is important to remember that "a cookie can be read only by HTML pages that sit on the same Web server and in the same directory as the page that set the cookie."[38] With the proper code, Target's cookie was "readable" by all of Smith's Web pages.[39]

II. Technical and Legal Aspects of Recent Cases Involving Cookies

To place this Note's legal analysis in context, it is essential to examine previous litigation over the use of cookies under the Stored Communications Act, the CFAA, and the Wiretap Act. This litigation has focused exclusively on commercial entities' use of cookies.[40] The *659 technical and legal aspects of two of these cases, In re DoubleClick, Inc. Privacy Litigation and In re Pharmatrak, Inc., provide a framework for analyzing the potential causes of action against a private individual who uses cookies to obtain another's personal information.

A. In re DoubleClick, Inc. Privacy Litigation

In re DoubleClick, Inc. Privacy Litigation was a class action suit brought against DoubleClick, "the largest provider of Internet advertising products and services in the world."[41] DoubleClick is an "intermediary" between host websites and the websites that place banner advertisements on the host websites.[42] It serves its clients by placing clients' banner advertisements before users who are within the client's "demographic target."[43] To accomplish this, DoubleClick utilizes user profiles and a process that is not visible to the user.[44] When a user visits the website of a DoubleClick client, a cookie is placed on the user's hard drive.[45] The next time the user accesses the client's website, the website sends its homepage and also sends a link to DoubleClick's server.[46] The resulting communication with DoubleClick's server includes information such as the "cookie identification number."[47] "[T]he DoubleClick server identifies the user's profile by the cookie identification number and runs a complex set of algorithms . . . to determine which advertisements it will present to the user."[48] DoubleClick sends the target banner ads and modifies the user's profile to reflect the latest request.[49]

*660 DoubleClick only collected user information when the users visited affiliated websites.[50] This information was only collected from GET, POST, and GIF information, not from the users' hard drives.[51] Additionally, DoubleClick did "not collect information from any user who [took] simple steps to prevent [its] tracking."[52]

The United States District Court for the Southern District of New York dismissed each of the plaintiffs' three statutory claims.[53] The claim under the Stored Communications Act failed on two grounds. First, the cookies and the identification numbers were not in "electronic storage" within the meaning of the Act, and therefore, were not within its scope.[54] Second, even if electronic storage requirement was satisfied, DoubleClick's actions fell within the Act's exception because the cookies and identification numbers were "'of or intended for"' DoubleClick.[55] The CFAA claim was unsuccessful because the plaintiffs were unable to meet the damages threshold required by the Act.[56] The plaintiffs' claim under the Wiretap Act also failed because DoubleClick's actions fell within the exception to the Wiretap Act; the affiliated websites were parties to the communication from the computer users and gave "sufficient

consent to DoubleClick to intercept" the cookies.[57] Further, the plaintiffs did not allege that DoubleClick acted with the criminal or tortious purpose required to invalidate the application of the statutory exception.[58]

B. In re Pharmatrak, Inc. Privacy Litigation

In re Pharmatrak, Inc. was a class action lawsuit brought by Internet users against Pharmatrak and the pharmaceutical companies to which it sold NETcompare.[59] The purpose of NETcompare was to "record the webpages a user viewed at clients' websites; how long the user spent on each webpage; the visitor's path through the site . . . the visitor's IP address; and . . . the webpage the user viewed immediately before arriving at the client's site."[60] However, NETcompare's purpose was not to collect *661 personal information.[61] To use NETcompare, a pharmaceutical client added "five to ten lines of HTML code to each webpage it wished to track and configure[ed] the pages to interface with Pharmatrak's technology."[62] Consequently, when a person visited a Pharmatrak client's Website, "Pharmatrak's HTML code instructed the user's computer to contact Pharmatrak's web server and retrieve from it a . . . 'clear GIF' (or a 'web bug')."[63] The clear GIF caused "the user's computer to communicate directly with Pharmatrak's web server."[64] During the user's first visit to a NETcompare website, the cookie was placed on the user's computer; during return visits to the website, Pharmatrak's servers would access the data on the cookie.[65]

The United States Court of Appeals for the First Circuit reversed the district court's finding under the Wiretap Act, holding that neither Pharmatrak's clients nor the computer users gave the consent required to bring Pharamatrak's actions under the statutory exception.[66] The First Circuit did not, however, address the district court's grant of summary judgment to the defendants on the Stored Communications Act and CFAA claims.[67] The district court found that the defendants were entitled to summary judgment on the Stored Communications Act claim because, inter alia, Pharmatrak's actions fell within the statutory exception.[68] Further, the district court found that the defendants were entitled to summary judgment on the CFAA claim because the plaintiffs had failed to meet the damages threshold.[69]

III. The Unlikelihood of Success of Claims Under the Stored Communications Act, the CFAA, and the Wiretap Act

Smith used cookies to access Target's personal information. Feeling that his privacy had been invaded, Target brought federal statutory claims under the Stored Communications Act, the CFAA, and the Wiretap Act. All three causes of action are doomed to fail, either because Target will be unable to satisfy the statutory requirements, or because Smith's conduct will fall within a statutory exception.

*662 A. Title II of the Electronic Communications Privacy Act--The Stored Communications Act

The purpose of the Stored Communications Act[70] was to "provide a cause of action against computer hackers."[71] When Congress passed the Act in 1986, it intended to "prevent[ ] computer hackers from obtaining or destroying electronic communications that were stored incident to their transmission."[72] The Stored Communications Act states that

[e]xcept as provided in subsection (c) of this section whoever--(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section."[73]

Pursuant to section 2707(a), an individual "aggrieved" by a violation of the Stored Communications Act may bring a civil claim.[74] However, under the statutory exception, there is no liability for "conduct authorized . . . by a user of that service with respect to a communication of or intended for that user."[75]

Claims under the Stored Communications Act challenging the commercial use of cookies have been unsuccessful.[76] While plaintiffs have been able to satisfy several of the claim's requirements, courts have generally held that the electronic storage requirement, located in section 2701(a)(2), or the statutory exception, located in section 2701(c)(2), relieve commercial entities using cookies of liability.[77] Pursuant to the analysis *663 used in the commercial cases, while Target will meet some of the statutory requirements, his claim under the Stored Communications Act will not succeed.

Under section 2701(a)(1), the defendant must have unlawfully accessed "a facility through which an electronic communication service is provided."[78] A personal computer qualifies as a facility for the purposes of the Act.[79] This requirement will be satisfied in Target's case because Target's personal computer made Smith's intrusion possible.[80] An electronic communications service, as required by section 2701(a), is defined in section 2510(15) as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[81] DoubleClick identified the Internet access provided by an Internet Service Provider as the requisite electronic communications service.[82] Target will satisfy this requirement because without Internet access he would have been unable to get online, read Smith's e-mails, and thereby access Smith's website.[83]

The Stored Communications Act's electronic storage requirement has generated considerable judicial attention.[84] The Act defines electronic storage as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[85] The DoubleClick court understood the term to apply to "electronic communications stored 'for a limited time' in the 'middle' of a transmission."[86] Consistent with this interpretation, the legislative history*664 for the Stored Communications Act refers exclusively to facilities like "'electronic bulletin boards' and 'computer mail facilit[ies],' and the risk that communications temporarily stored in these facilities could be accessed by hackers."[87] To buttress its interpretation, the court in DoubleClick observed that if the cookies in that case were found to be in electronic storage, websites would be committing a crime with every access of a cookie, irrespective of the type of information stored on the cookie.[88]

Target is unlikely to satisfy the electronic storage requirement. Because the DoubleClick plaintiffs alleged that the cookies remained on their hard drives indefinitely, the court held that they were not in electronic storage as contemplated by the Stored Communications Act.[89] Similarly, the cookies sent from Smith's webpage will most likely be persistent cookies and will

be meant to remain on Target's computer indefinitely.[90] In any case, there is really no way to interpret the cookies as "stored for a 'limited time' in the 'middle' of a transmission," as required by the DoubleClick court, because even per session cookies will not expire until "the browser is closed" or "a set expiration time."[91] Therefore, because Target will be unable to meet this requirement, his claim under the Stored Communications Act will fail.

Even if Target meets the statutory requirements of the Stored Communications Act, his claim will fail under the Act's exception, which provides that the statutory prohibition will not apply "with respect to conduct authorized . . . by a user of that service with respect to a communication of or intended for that user."[92] Courts have found the use of cookies lawful in commercial cases because they have qualified under this exception.[93] To meet the exception's requirements, the use of cookies must be authorized by a user of an electronic communications service and the communication must be "intended for that user."[94] Users may include individuals using Internet access, websites, and servers.[95] The DoubleClick *665 court classified the websites affiliated with DoubleClick as users within the meaning of the Stored Communications Act.[96] The cookies' information was found to be intended for these affiliated sites, because website visitors "voluntarily type-in information they wish to submit to the [w]ebsites."[97] Further, these affiliated websites then authorized DoubleClick to have access to the information in the cookies.[98]

In the hypothetical case, Smith's conduct will fall within the exception. Whether Smith is classified as an individual using the Internet or the operator of a website or server, he will qualify as a "user" under the Stored Communications Act.[99] Further, like the plaintiffs in DoubleClick, because Target voluntarily gave information to Smith's website, his transmission was intended for Smith's website.[100] There is no authorization issue as there was in DoubleClick[101] because Smith alone accessed the information.

Therefore, Target's claim against Smith under the Stored Communications Act will fail, either because Target will fail to meet the requirements of the statute or because Smith's conduct will fall within the statutory exception.

B. The Computer Fraud and Abuse Act

There are two relevant provisions of the CFAA.[102] First, the act prescribes punishment for one who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer if the conduct involved an interstate or foreign communication."[103] Second, the CFAA prohibits one from "knowingly caus[ing] the transmission of a program, information, *666 code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer."[104]

The CFAA provides for a civil cause of action in section 1030(g).[105] However, to state a cause of action for the use of cookies under the CFAA, the plaintiff must allege a threshold of economic damages, set at $5,000, pursuant to section 1030(a)(5)(B)(i).[106] This threshold requirement has consistently led to the dismissal of claims challenging the use of cookies and will most likely mandate the same result for Target's CFAA claim.[107]

The CFAA was amended in 2001 when Congress wrote the Patriot Act.[108] Under amended section 1030(g), to satisfy the $5,000 threshold set forth in section (a)(5)(B)(i), a plaintiff must allege economic damages.[109] Even before the 2001 amendment, despite some confusion over the previous statutory language, courts applied the economic damages requirement to the $5,000 threshold.[110] For example, in DoubleClick, the District Court for the Southern District of New York quoted a 1996 Senate *667 Report, which stated that "'damages recoverable in civil actions by victims of computer abuse would be limited to economic losses for violations causing losses of $5,000 or more during any 1-year period.'"[111] Further, economic damages may only be calculated based on a "single act or event."[112]

The DoubleClick court found that plaintiffs could meet the threshold with by showing any economic losses they suffered in securing or remedying their systems.[113] In that case, however, the court found that because the plaintiffs failed to plead that DoubleClick "caused any damage whatsoever to plaintiffs' computers, systems or data that could require economic remedy," if there were economic damages at all, they were "insignificant."[114] The Avenue A court was perhaps the most concise when it stated that "[u]nlike a computer hacker's illegal destruction of computer files or transmission of a widespread virus which might cause substantial damage to many computers as the result of a single act . . . the transmission of an internet cookie is virtually without economic harm."[115] In fact, that court noted the Congress intended to punish "only the most severe of computer fraud actions."[116]

The threshold requirement will most likely defeat Target's CFAA claim. When Smith accessed information from Target's cookies, none of Target's computer files were destroyed and he did not receive a virus.[117] Any financial loss incurred by Target would be minimal. By analogy, the DoubleClick court found that the plaintiffs failed to plead damages meeting the required threshold when they sought damages for "an invasion of their privacy, a trespass to their personal property, and the misappropriation of confidential data."[118] Therefore, because Target will most likely fail to incur substantial economic losses totaling at least $5,000 as a result of *668 Smith's use of cookies, Target will be unable to maintain a cause of action under the CFAA.

C. Title I of the Electronic Communications Privacy Act--The Wiretap Act[119]

"The paramount objective of the Wiretap Act is to protect effectively the privacy of communications."[120] In 1986, the Electronic Communications Privacy Act amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[121] This amendment gave data and electronic transmissions the same protection the original Act granted to oral and wire communications.[122] In Konop v. Hawaiian Airlines, Inc., a case regarding a secure Website, the Ninth Circuit remarked that the "ECPA was written prior to the advent of the Internet and the World Wide Web. . . . Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results."[123]

The Wiretap Act's general prohibition states that

[e]xcept as otherwise specifically provided in this chapter any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to

intercept, any wire, oral, or electronic communication . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).[124]

The elements of the Wiretap Act require that a "defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device."[125] Under the analysis of previous cases dealing with the use of cookies, specifically Pharmatrak, Target is likely to satisfy the requirements for a claim under the Wiretap Act.

To prove that a defendant had the requisite state of mind, the "conduct or the causing of the result must have been the person's conscious *669 objective."[126] When Congress amended the ECPA in 1986, it emphasized that "inadvertent interceptions" are not enough for liability under the Wiretap Act.[127] Accordingly, the Pharmatrak court noted that the intent requirement will most likely be satisfied where the conduct "serves a party's self-interest."[128] In the hypothetical case, Smith's acquisition of the information on Target's cookies was anything but inadvertent.[129] In fact, it served both Smith and Victim's self-interests.[130] Smith stood to gain a fee from Victim, who had an incentive to end the stalking and potentially save his own life and that of his family.

Under the Wiretap Act, interception is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device."[131] This requirement will only be satisfied if the acquisition of electronic communications occurs "contemporaneously with their transmissions."[132] In Pharmatrak, interception occurred because Pharmatrak's acquisition of the cookies was "contemporaneous with the transmission by the internet users to the pharmaceutical companies."[133] Target will be able to satisfy this requirement. In Pharmatrak, the court found the interception element was met, even though there was a third party involved, specifically, Pharmatrak.[134] In the hypothetical situation, Target's electronic communications were sent only to Smith's server and needed to go no further.[135]

*670 Under the Wiretap Act, the contents which must have been intercepted for the claim to succeed "include[] any information concerning the substance, purport, or meaning of that communication."[136] The definition of the term contents includes "personally identifiable information such as a party's name, date of birth, and medical condition."[137] In Target's case, personal information was the sole item Smith was seeking. In fact, Smith and Victim implemented the cookies with the express purpose of discovering the name of the person sending threatening emails, which they succeeded in doing.

The ECPA adopts a "'broad, functional' definition of an electronic communication," which must be satisfied to prove a claim under the Wiretap Act.[138] An electronic communication is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system that affects interstate . . . commerce."[139] This definition is subject to four exceptions.[140] The Pharmatrak court determined that "[t]ransmissions of completed online forms . . . constitute electronic communications."[141] In the hypothetical, Smith obtained Target's personal information when Target registered with Smith's Website using "multiple blank fields."[142]

Finally, Web servers may be used to satisfy the device requirement.[143] Smith was able to acquire the cookies using his own server. In fact, only Smith's server could read the information contained in Target's cookies.[144]

Although Target will be able to meet the requirements for a cause of action under the Wiretap Act, Smith's conduct will likely fall within the statutory exception. This exception states:

[i]t shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any *671 criminal or tortious act in violation of the Constitution or laws of the United States or of any State.[145] The burden of proving the exception is on the party seeking its benefit.[146] Essentially, this party must prove that a party to the communication consented to the interception.[147]

To determine whether the exception applies, a court must determine whether the Website sending and intercepting the cookies was "a party to the communication."[148] Courts analyzing the use of cookies have found that Websites using the services of DoubleClick and Avenue A were parties to the communication.[149] In fact, the DoubleClick court analogized parties to the communication under the Wiretap Act to users under the Stored Communications Act, a definition which includes Websites and Web servers.[150] Either Smith or his Website will therefore qualify as a party to the communication.[151]

Further, the DoubleClick and Avenue A courts found that these affiliated Websites, as parties to the communication, consented to the interception of information in the users' cookies.[152] Both courts reasoned that the consent requirement was directly analogous to the authorization requirement of the Stored Communications Act, which both found to have been satisfied.[153] The DoubleClick court justified its interpretation of the statute by noting that "courts have emphasized that 'consent' must be construed broadly under the Wiretap Act."[154] Under this analysis, Smith, a party to the communication, consented to the interception of the information in Target's cookies.[155] In fact, Smith initiated the use of cookies in this situation and engineered the acquisition of Target's personal *672 information. Because "[o]ne-party consent is sufficient to negate liability" under the Wiretap Act,[156] this consent brings Smith's conduct within the statutory exception.

This statutory exception will not apply, however, where the communication "is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State."[157] The determinative question in this analysis is whether the "purpose for the interception--its intended use--was criminal or tortious."[158] Essentially, there is a difference between tortious purpose and tortious means.[159] Further, in order to defeat the exception, the plaintiff must show that the tortious or criminal purpose was the "primary motivation" or a "determinative factor in the actor's . . . motivation for intercepting" the communication.[160]

For example, the requisite purpose was lacking in DoubleClick.[161] There was no evidence that DoubleClick obtained the plaintiff's cookies with an "'insidious' intent to harm plaintiffs or

others."[162] Instead, DoubleClick was "consciously and purposefully executing a highly-publicized market-financed business model in pursuit of commercial gain--a goal courts have found permissible" under this exception.[163] Consistent with this interpretation, the Court of Appeals for the Ninth Circuit noted in Sussman v. American Broadcasting Cos., Inc. that interception for the purposes of news gathering would not have the required tortious or criminal purpose.[164] However, that court also provided examples of situations in which the required purpose would be present.[165] Specifically, there would be an illegitimate purpose where a news agency intercepted communications with the purpose of "airing private intimate *673 conduct" or where the interception was performed to facilitate blackmail.[166]

Here, the primary motivation[167] behind the interception was determining the true identity of the stalker. The purpose was not to expose any of the confidential information Target had stored on his computer or to air his "private intimate conduct."[168] Especially given the dire circumstances brought on by the stalking, Victim and Smith's objectives seem more consistent with news gathering than with blackmail.[169] Because there is no evidence to suggest that Smith's purpose was unlawful, the exception will apply to his conduct.[170]

Therefore, while Target will satisfy the requirements of the Wiretap Act, Smith's use of cookies will fall under the Act's exception and Smith will be able to escape civil liability.

Conclusion

Based on the foregoing analysis, Target and others like him will be unable to bring successful claims under the Stored Communications Act, the CFAA, or the Wiretap Act.
…
The author submits that the best suggestion would be to provide a specific federal cause of action for victims of private individuals who use cookies to obtain personal information. Until such legislation is passed, or an alternative solution is presented, victims like Target will be legally helpless against private individuals well-versed in cookies' capabilities.

Footnotes

1. See, e.g., In re Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001); Yochi J. Dreazen, The Best Way To... ... Guard Your Privacy, Wall St. J., Nov. 18, 2002, at R4.
2. See, e.g., In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9 (1st Cir. 2003); In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001); In re Toys R Us, Inc., Privacy Litig., No. 00-2746, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001).
3. See DoubleClick, 154 F. Supp. 2d at 500; Avenue A, 165 F. Supp. 2d at 1155;Toys R Us, 2001 U.S. Dist. LEXIS 16947, at *6, 19, 28.
4. 18 U.S.C. § 2511 (2000), amended by, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, §§ 204, 217, 115 Stat. 272, 281, 292 (2001); Homeland Security Act of 2002, Pub. L. No. 107-296, § 225,116 Stat. 2135, 2158 (2002).
5. 18 U.S.C. § 2701 (2000), amended by, Homeland Security Act of 2002, Pub. L. No. 107-296, § 225, 116 Stat. 2135, 2158 (2002).
6. 18 U.S.C. § 1030 (2000), amended by Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, §

814, 115 Stat. 272, 366, 382 (2001). One year later, Congress amended this section in the Cyber Security Enhancement Act of 2002. Homeland Security Act of 2002, Pub. L. No. 107-296, § 225(g), 116 Stat. 2135, 2158 (2002).
…
30. Id. at 649-50.
31. Id. at 650.
32. Id. at 649.
33. Id. at 650.
34. Id.
35. See Mark Sweiger, Cookies: The Perfect User Identification Snack, Clickstream Consulting, at http://www.clickstreamconsulting.com/article06.html (last visited Jan. 19, 2005).
36. Id.
37. See supra note 15 and accompanying text.
38. Thau, Advanced Javascript Tutorial Lesson 2, at 13, Lycos, at http://hotwired.lycos.com/webmonkey/98/29/index1a_page13.html?tw=programming (last visited Jan. 19, 2005); see also Sweiger, supra note 35.
39. See Thau, supra note 38.
40. See, e.g., In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9 (1st Cir. 2003); In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001); In re Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001). In an article profiling Lou Montulli, the creator of cookies, Thomas Weber examined the reasons commercial websites began to use cookies. Weber, supra note 8. He notes that "[w]hen Websites began to run paid advertisements, advertisers wanted to know the size of the audience." Id. It was impossible to determine whether multiple "hits" signified multiple users visiting once, or the same user visiting multiple times. Id. The process of assigning cookies to visitors allowed websites to "discern one visitor from another and make accurate tallies." Id. After accomplishing this, "it wasn't much of a leap to use cookies to track visitors' habits." Id.
41. In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001). The relevant facts of Chance v. Avenue A, Inc. are very similar to those in DoubleClick.Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1156 (W.D. Wash. 2001). Avenue A also "serves as an intermediary," working with host and advertising websites using banner advertisements. Id. When the user's browser accesses the webpage in question, a link instructs "the user's computer to send a communication automatically to Avenue A's server" which identifies the computer's cookie. Id. "Avenue A's server analyzes its cookie and sends an advertisement targeted at what it believes to be the user's preferences." Id.
42. DoubleClick, 154 F. Supp 2d. at 502.
43. Id. "DoubleClick, which sells advertising on a network of sites, figured it could charge more for ads if they were targeted based on consumer behavior." Weber, supra note 8.
44. DoubleClick, 154 F. Supp. 2d at 502, 504.
45. Id. at 502-03.
46. Id. at 503.
47. Id.
48. Id.
49. Id. at 503-04.
50. Id. at 504.
51. Id.
52. Id.
53. Id. at 514, 519, 526.
54. Id. at 511.
55. Id. at 513.
56. Id. at 526.
57. Id. at 514.

58. Id. at 519.
59. In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 12 (1st Cir. 2003).
60. Id. at 13.
61. Id.
62. Id.
63. Id. at 13-14.
64. Id. at 14.
65. Id.
66. Id. at 19-21, 23.
67. Id. at 17; In re Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 15 (D. Mass 2002).
68. Pharmatrak, 220 F. Supp. 2d at 13.
69. Id. at 15.
70. 18 U.S.C. § 2701 (2000).
71. State Wide Photocopy, Corp. v. Tokai Fin. Servs., Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995).
72. Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1160 (W.D. Wash. 2001).
73. 18 U.S.C. § 2701(a).
74. Id. § 2707(a).
Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate. Id.; see also In re Toys R Us, Inc., Privacy Litig., No. 00-1381, 2001 U.S. Dist. LEXIS 16947, at *7 (N.D. Cal. Oct. 9, 2001).
75. 18 U.S.C. § 2701(c)(2).
76. See, e.g., Toys R Us, 2001 U.S. Dist. LEXIS 16947, at *18; Avenue A, 165 F. Supp. 2d at 1162; In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 513-14 (S.D.N.Y. 2001).
77. See Avenue A, 165 F. Supp. 2d at 1162; DoubleClick, 154 F. Supp. 2d at 513.
78. 18 U.S.C. § 2701(a)(1).
79. Avenue A, 165 F. Supp. 2d at 1161. The Avenue A court found that "[v]iewing this factual dispute in the light most favorable to the nonmovant [the defendant]... it is possible to conclude that modern computers... are facilities covered under the Act." Id. In Toys R Us, the United States District Court for the Northern District of California rejected the defendant's argument that a "'facility' cannot refer to a personal computer." 2001 U.S. Dist. LEXIS 16947, at *8 n.7. That court explained that other cases have "rejected, either expressly or implicitly" the defendant's interpretation, using the DoubleClick case as an example. Id. But see In re Pharmatrak, Inc. Privacy Litig., 220 F. Supp. 2d 4, 13 (D. Mass. 2002) (finding that the plaintiffs' "personal computer is not a 'facility"' within the meaning of the Act).
80. See 18 U.S.C. § 2701(a)(1); Avenue A, 165 F. Supp. 2d at 1161.
81. 18 U.S.C. § 2510(15).
82. DoubleClick, 154 F. Supp. 2d at 508.
83. See id.
84. 18 U.S.C. § 2701(a)(2); see, e.g., DoubleClick, 154 F. Supp. 2d at 511-13.
85. 18 U.S.C. § 2510(17)(A). Section 2510(17)(B) also defines this term as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." Id. § 2510(17)(B). However, the plaintiffs in the relevant cases and in this hypothetical are not electronic communications services. Toys R Us, 2001 U.S. Dist. LEXIS 16947, at *9 n.9.
86. DoubleClick, 154 F. Supp. 2d at 512.
87. Id. at 512 (quoting S. Rep. No. 99-541 (1986)).
88. Id. at 512-13.
89. Id.
90. See supra Part I.A,
91. DoubleClick, 154 F. Supp. 2d at 512; McClure, supra note 17 at 649.

92. 18 U.S.C. § 2701(c)(2).
93. DoubleClick, 154 F. Supp. 2d at 511; Toys R Us, 2001 U.S. Dist. LEXIS 16947, at *18; Avenue A, 165 F. Supp. 2d at 1161.
94. 18 U.S.C. §§ 2701(c)(1)-(2); see also Avenue A, 165 F. Supp. 2d at 1161.
95. DoubleClick, 154 F. Supp. 2d at 509. The court in DoubleClick noted that "in a practical sense, [w]ebsites are among the most active 'users' of Internet access." Id. A user is defined under the Act as "any person or entity who [ ] uses an electronic communications service; and is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13).
96. DoubleClick, 154 F. Supp. 2d at 509; see also Avenue A, 165 F. Supp. 2d at 1161.
97. DoubleClick, 154 F. Supp. 2d at 511 (emphasis added). Further, even when the users request information "through clicks [of a mouse], not keystrokes," this is "voluntary and purposeful." Id.
98. Id.; see also Avenue A, 165 F. Supp. 2d at 1161. The Avenue A court noted that "[g]iven the technological and commercial relationship between websites and Avenue A, it is implausible to suggest that any such 'access' by Avenue A was not intended or authorized by the website." Id. "In fact... the very raison d'etre of Avenue A is to provide websites with targeted advertising, and it cannot do so without the collaboration and consent of those sites." Id.
99. See DoubleClick, 154 F. Supp. 2d at 509.
100. See id. at 511.
101. Id. at 510.
102. 18 U.S.C. § 1030 (2000), amended by Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107-56, § 814, 115 Stat. 272, 382-84 (2001).
103. 18 U.S.C. § 1030(a)(2)(C); see also Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1160, 1158 (W.D. Wash. 2001).
104. 18 U.S.C. § 1030(a)(5)(A)(i); see also Avenue A, 165 F. Supp. 2d at 1158.
105. 18 U.S.C. § 1030(g).
106. Id. § 1030(g), (a)(5)(B)(i); see also Avenue A, 165 F. Supp. 2d at 1158. Section 1030(g) of the CFAA provides that "[a] civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving conduct described in subsection (a)(5)(B)(i) are limited to economic damages." 18 U.S.C. § 1030 (g). The relevant factors of section 1030(a)(5)(b) are:
[L]oss to 1 or more persons during any 1-year period... aggregating at least $5,000 in value; the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; physical injury to any person; a threat to public health or safety; or damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security."
Id. § 1030(a)(5)(B)(i)-(v). The author submits that, given the hypothetical context of this Note, subsection (a)(5)(B)(i) is the only relevant factor in this analysis.
107. See Avenue A, 165 F. Supp. 2d at 1160; In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001).
108. USA Patriot Act § 814. Due to the recent amendment, the statutory context of our hypothetical plaintiff's CFAA claim will differ from previous cookies cases in a manner worth mentioning, but which will not affect the outcome of the analysis. Prior to 2001, the damage requirement was governed by section 1030(e)(8) of the CFAA, which defined "damage" as "any impairment to the integrity or availability of data, a program, a system, or information, that ... causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals." 18 U.S.C. § 1030(e)(8) (before 2001 amendment). In 2001, Congress amended the CFAA when it wrote the Patriot Act. The Patriot Act made the threshold damages requirement correlative with section 1030(a)(5)(B), instead of (e)(8). USA Patriot Act § 814; Computer Fraud and Abuse Act §§ 1030(g), 1030(a)(5)(B)(i).
109. 18 U.S.C. §§ 1030(g), 1030(a)(5)(B)(i).

110. DoubleClick, 154 F. Supp. 2d at 520-22; Avenue A, 165 F. Supp. 2d at 1160-61; In re Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. LEXIS 16947, at *32 (N.D. Cal. Oct. 9, 2001).
111. DoubleClick, 154 F. Supp. 2d at 521 (quoting S. Rep. No. 104-357 (1996)(emphasis added by court)).
112. Avenue A, 165 F. Supp. 2d at 1158-59. Prior to the 2001 amendment, courts interpreting the word "impairment" in section 1030(e)(8) held that the damages must have arisen out of a "single act or event." Id. at 1158; DoubleClick, 154 F. Supp. 2d at 523. The United States District Court for the Western District of Washington, in Avenue A, found that "each time a web page sends a message to a user's computer instructing the computer to communicate the contents of the cookie on the user's hard drive... it is an individual, singular act." Avenue A, 165 F. Supp. 2d at 1159. The current version of section 1030(e)(8) preserves the "impairment" language. 18 U.S.C. § 1030(e)(8).
113. DoubleClick, 154 F. Supp. 2d at 524; see also Avenue A, 165 F. Supp. 2d at 1160.
114. DoubleClick, 154 F. Supp. 2d at 525.
115. Avenue A, 165 F. Supp. 2d at 1159.
116. Id. at 1160.
117. See id. at 1159.
118. DoubleClick, 154 F. Supp. 2d at 523.
119. 18 U.S.C. § 2511 (2000).
120. In re Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 18 (1st Cir. 2003).
121. Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460 (5th Cir. 1994).
122. Pharmatrak, 329 F.3d at 18.
123. 302 F.3d 868, 874 (9th Cir. 2002); see also United States v. Councilman, 373 F.3d 197, 203 (1st Cir. 2004) (noting that "[i]t may well be that the protections of the Wiretap Act have been eviscerated as technology advances").
124. 18 U.S.C. § 2511(1)(a) (2000).
125. Pharmatrak, 329 F.3d at 18.
126. Id. at 23 (quoting S. Rep. No. 99-541, at 23 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3577).
127. Id.
128. Id.
129. See id.
130. See id.
131. 18 U.S.C. § 2510(4).
132. Wesley Coll. v. Pitts, 974 F. Supp. 375, 385 (D. Del. 1997). When Congress passed the Patriot Act it "accepted and implicitly approved the judicial definition of 'intercept' as acquisition contemporaneous with transmission." Konop, 302 F.3d at 878.
133. Pharmatrak, 329 F.3d at 22. The First Circuit, in United States v. Councilman, noted that in Pharmatrak "[t]he messages were not placed in any type of storage before their interception, therefore skirting the 'contemporaneous' problem." 373 F.3d at 201 n.6.
134. 329 F.3d at 22. The court explained that "NETcompare was effectively an automatic routing program. It was code that automatically duplicated part of the communication between a user and a pharmaceutical client and sent this information to a third party (Pharmatrak)." Id. Pharmatrak's argument that interception was impossible because there were "'two separate communications,"' was rejected. Id. The court held that "[s]eparate, but simultaneous and identical, communications satisfy" the interception requirement. Id.
135. See id.
136. 18 U.S.C. § 2510(8).
137. Pharmatrak, 329 F.3d at 18.
138. Id. (quoting Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995)).
139.18 U.S.C. § 2510(12).
140. Id.
141. Pharmatrak, 329 F.3d at 18.

142. See In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 504 (S.D.N.Y. 2001)504; see also supra Part I.A.
143. Pharmatrak, 329 F.3d at 19.
144. See Microsoft, supra note 12.
145. 18 U.S.C. § 2511(2)(d).
146. Pharmatrak, 329 F.3d at 19.
147. 18 U.S.C. § 2511(2)(d).
148. Id.; see also DoubleClick, 154 F. Supp. 2d at 514.
149. Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1160, 1162 (W.D. Wash. 2001);DoubleClick, 154 F. Supp. 2d at 514.
150. DoubleClick, 154 F. Supp. 2d at 509, 514.
151. See id.
152. Avenue A, 165 F. Supp. 2d at 1161-62; DoubleClick, 154 F. Supp. 2d at 511, 514.
153. Avenue A, 165 F. Supp. 2d at 1161-62; DoubleClick, 154 F. Supp. 2d at 511, 514. The First Circuit in Pharmatrak found a lack of consent. Pharmatrak, 329 F.3d at 20-21. However, that case is distinguishable from both the referenced commercial cases and the hypothetical Wiretap claim. There, "[f]ar from consenting to the collection of personally identifiable information, the pharmaceutical clients explicitly conditioned their purchase of NETcompare on the fact that it would not collect such information.... Nor did the users consent." Id. at 20-21 (emphasis added).
154. DoubleClick, 154 F. Supp. 2d at 514 n.23.
155. See Avenue A, 165 F. Supp. 2d at 1161-62; DoubleClick, 154 F. Supp. 2d at 511, 514.
156. Avenue A, 165 F. Supp. 2d at 1162.
157. 18 U.S.C. § 2511(2)(d).
158. Sussman v. Am. Broadcasting Cos., Inc., 186 F.3d 1200, 1202 (9th Cir. 1999)(emphasis added) (quoting Payne v. Norwest Corp., 911 F. Supp. 1299, 1304 (D. Mont. 1995)).
159. Avenue A, 165 F. Supp. 2d at 1162. In Sussman, the Ninth Circuit held that the Wiretap Act only prohibits a tortious or criminal purpose, stating that "[w]here the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere." 186 F.3d at 1202-03.
160. DoubleClick, 154 F. Supp. 2d at 514-15 (quoting United States v. Dale, 991 F.2d 819, 841-42 (D.C. Cir. 1993)).
161. Id. at 519.
162. Id. at 518.
163. Id.
164. 186 F.3d at 1202.
165. Id.
166. Id. at 1202-03.
167. See DoubleClick, 154 F. Supp. 2d at 514-15 (quoting Dale, 991 F.2d at 841-42).
168. See Sussman, 186 F.3d at 1202.
169. See id.
170. See Avenue A, 165 F. Supp. 2d at 1163.
…

To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising

Omer Tene & Jules Polonetsky
Minnesota Journal of Law, Science & Technology
Volume: 13
Starting Page: 281, 283
2012

V. PROPOSALS FOR REGULATORY REFORM

The past year featured a burst of activity in Washington ***320** focused on both online and offline privacy regulatory reform. It has been anchored by the FTC Preliminary Report, followed by a swift response from industry, and reinvigorated by a slew of legislative bills.[189] It included the creation for the first time of a dedicated Senate Sub-Committee on Privacy, Technology and the Law, headed by Senator Al Franken (D-MN) and charged with "[o]versight of laws and policies governing the collection, protection, use, and dissemination of commercial information by the private sector, including online behavioral advertising."[190]

A. The FTC Do Not Track Proposal

The FTC Preliminary Report sets forth three central axes for future regulation of online privacy: First, privacy by design, according to which companies should promote privacy protections throughout the organization and at every stage of the development of products and services starting at the design phase; such protections should include providing data security; collecting only the data required for a specific business purpose (data minimization); retaining data only long enough to fulfill that purpose (retention limitation); and ensuring reasonable data accuracy (data quality).[191]

Second, simplified choice, meaning that on the one hand, companies need not provide choice before collecting and using data for "commonly accepted" practices such as product fulfillment, internal operations, fraud prevention, legal compliance, and first-party marketing; on the other hand, for practices requiring choice, companies must offer choice at a time and in a context in which the user is making a decision about her data, and implement a DNT mechanism for online behavioral advertising.[192]

***321** Third, increased transparency, calling for privacy notices to be clearer, shorter, and more standardized; for companies to provide reasonable access to any data they maintain, in proportion to the sensitivity of the data and the nature of their use; and for companies to provide prominent disclosures and obtain affirmative express consent before using data in a manner materially different from that presented at the time of collection.[193]

Most of the public debate following the FTC's Preliminary Report focused on the DNT proposal for compliance with a user's centralized opt-out of online behavioral tracking.[194] The FTC

contemplates that DNT could be advanced by either legislation or enforceable industry self-regulation.[195] It states that:

> [t]he most practical method of providing uniform choice for online behavioral advertising would likely involve placing a setting similar to a persistent cookie on a consumer's browser and conveying that setting to sites that the browser visits, to signal whether or not the consumer wants to be tracked or receive targeted advertisements. To be effective, there must be an enforceable requirement that sites honor those ***322*** choices.[196]

In addition, the FTC stresses that DNT differs from Do Not Call in that it will not necessitate a central registry, instead relying on a browser-based mechanism through which users could make persistent choices.[197]

Even before implementing DNT, most online behavioral tracking companies offer end users the option to opt-out of tracking cookies.[198] Such an opt-out typically relied on the users clicking to accept an opt-out cookie.[199] However, opt-out cookies were often deleted when users cleared their cookie folder, tossing such users unknowingly back into the ad targeting pool.[200] In addition, the lack of a well-known central location for opting-out required users to review privacy policies in order to discover links to opt-out tools.[201] Finally, the FTC noted: "existing mechanisms may not make clear the scope of the choices being offered. It may not be clear whether these mechanisms allow consumers to choose not to be tracked, or to be tracked but not delivered targeted advertising."[202] Hence, a robust DNT mechanism must clarify to users not only how they can exercise their opt-out right but also what exactly they are opting-out of? Is it data collection or only ad targeting? And what exactly does "tracking" mean in this context?

B. Industry Proposals

Before drawing FTC support, DNT was an advocacy group initiative, submitted during an FTC workshop on behavioral advertising in October 2007.[203] The privacy group proposed: "To help ensure that [the privacy] principles are followed, the FTC ***323*** should create a national Do Not Track List similar to the national Do Not Call List."[204] The proposal would have required advertisers to submit their tracking domains to the FTC, which would make a DNT list available on its website for download by users who wish to limit tracking.[205] The idea remained dormant until July 2009, when privacy advocate Christopher Soghoian first developed his Targeted Advertising Cookie Opt-Out (TACO) mechanism as a prototype plug-in that automatically checks for a header on a website to determine whether to allow tracking cookies.[206] Version 4.40 of the TACO plug-in could block a total of 120 advertising networks; show granular detail on which tracking systems a website was using; and display them on a console when a user visits a new web page.[207] Further controls allowed users to block particular tracking systems while allowing others.[208] But the concept failed to resonate with the broader policy or advertising communities.[209] Soghoian and his research collaborator Sid Stamm later put together a prototype Firefox add-on that added a DNT header to outgoing HTTP requests, which is the precursor to the headers that are being implemented by industry today.[210]

DNT first gained momentum as a viable policy concept in July 27, 2010, when FTC Chairman Jon Leibowitz testified at the Senate Committee on Commerce, Science and Transportation on

efforts to protect consumer privacy.[211] Departing from ***324*** scripted remarks, Chairman Leibowitz stated that the FTC is calling for an industry-led DNT program.[212] Stanford researchers Jonathan Mayer and Arvind Narayanan followed suit by creating "donottrack.us" to provide "a web tracking opt-out that is user friendly, effective, and completely interoperable with the existing web."[213] Their approach, like Soghoian and Stamm's before them, depends on Internet browsers sending a header to permit the placement of tracking cookies on a user's computer.[214]

Initial industry response was hardly enthusiastic, declaring that "[i]f mandated by the government, this would be tantamount to a government-sponsored, and possibly managed, ad-blocking program--something inimical to the First Amendment."[215] DNT was seen as distraction from self-regulatory efforts organized by advertising industry groups, which were based on icons on behavioral ads leading to opt-out tools.[216] However, the release of the FTC's Preliminary Report in December 2010 prompted the major browser makers to engage with the DNT proposal.[217]

In December 2010, Microsoft implemented a "Tracking Protection" feature in its new Internet Explorer 9 browser, allowing users to select a Tracking Protection List (TPL) from a choice provided by various organizations, such as Abine, EasyList, PrivacyChoice, and TRUSTe.[218]Simply stated, a TPL contains web addresses that the browser will visit only if a user ***325*** typed in their address or linked to them directly.[219] Indirect access to a listed website is blocked, so if a web page contains links to other content from blocked addresses, such links are not visited and cookies from such website are blocked.[220] Microsoft states that the new feature provides "a new browser mechanism for consumers to opt-in and exercise more control over their browsing information. By default the Tracking Protection List is empty, and the browser operates just as it does today."[221] While presented as an opt-in mechanism, TPL is really an opt-out tool (which users may choose to opt-into).[222] Despite earlier skepticism about the concept, Microsoft also added a DNT browser header--which is automatically activated when a TPL (even an empty one) is uploaded--in its final release of Internet Explorer 9.[223]

Mozilla, maker of the Firefox browser, presented an approach based on a DNT browser header.[224] On January 23, 2011, Mozilla released Firefox 4, which allows users to check a "Do Not Track" box in the "advanced" settings of the browser, prompting a header to be sent with every click or page request signaling to websites that the user does not wish to be tracked.[225]Unlike Microsoft's TPL solution, the DNT header leaves it entirely up to receiving websites to honor the user's request by omitting any tracking cookies from their response.[226] As the CDT explains, "Firefox users will have to rely upon individual ***326*** websites to honor their 'Do Not Track' requests. Today, websites do not have the infrastructure to accommodate these requests . . . ."[227]

Google, maker of the Chrome browser, took a different approach, introducing the Keep My Opt-Outs plug-in, allowing users to permanently opt-out of online behavioral tracking by companies participating in self-regulatory programs.[228] The new plug-in was meant to remedy the recurrent problem whereby users cleared out any opt-out cookies when purging their cookie folder, thus unknowingly re-entering the tracking domain.[229] Keep My Opt-Outs is itself cookie based--it deletes all cookies sent by registered domains and adds a DNT cookie for such domains.[230]Apple

too added a DNT tool to a test version of its Safari browser included within the latest version of Lion, its new operating system.[231]

Each of the industry mechanisms for implementation of DNT has its own costs and benefits.[232]The FTC put forth the following criteria to assess industry efforts: DNT should be universal, that is, a single opt-out should cover all would-be trackers; easy to find, understand, and use; persistent, meaning that opt-out choices do not "vanish"; effective and enforceable, covering all tracking technologies; and controlling not only use of data but also their collection.[233] As discussed, the FTC ***327** has not yet taken a position on whether any legislation or rulemaking is necessary for DNT.[234] It is clear, however, that regardless of the regulatory approach chosen, industry collaboration will remain key since the system will only work if websites and ad intermediaries respect users' preferences.

C. Draft Legislation

The renewed public interest in privacy and online behavioral tracking, spurred by the Wall Street Journal "What They Know" series,[235] FTC and Department of Commerce engagement with the topic, and occasional front-page privacy snafu (e.g., Google Buzz,[236] iPhone location tracking[237]), has led to an unprecedented flurry of activity and legislative proposals on the Hill.[238] As discussed below, all bills address transparency and choice requirements, and several refer specifically to DNT.

1. The Best Practices Act

On July 19, 2010, House Representative Bobby Rush (D-IL) introduced a privacy bill, which would establish national requirements for collecting and sharing personal information, codifying certain fair information principles into law.[239] The bill mandates increased transparency, requiring covered entities to make specific privacy disclosures to individuals whose personal information they collect or retain "in concise, meaningful, timely, ***328** prominent, and easy-to-understand" fashion, with a special provision allowing the FTC to introduce standardized short-form notices that users are more likely to understand.[240] It requires that mechanisms be put in place to facilitate user choice, providing users with a "reasonable means" to opt-out of information collection and use for non-operational purposes;[241] however, businesses may explicitly condition a service on a user not opting-out of secondary usage.[242] The bill requires opt-in consent for: (1) the collection, use or disclosure of sensitive information, which includes medical history, race, ethnicity or religious beliefs, sexual orientation or sexual behavior, financial information, precise geo-location information, and biometric data;[243] (2) disclosure of covered information to third parties for non-operational purposes;[244] (3) any "material" changes to privacy practices governing previously collected information;[245] and (4) use of software or hardware "to monitor all or substantially all of an individual's Internet browsing" activity.[246]

To promote enforceable industry self-regulation, the bill would provide a "safe harbor" substituting opt-in consent requirements for opt-outs, where companies enroll in FTC-monitored and approved universal opt-out programs operated by industry self-regulatory programs ("Choice Programs").[247] Choice Programs would, at minimum, would be required to: (1) provide a clear and conspicuous opt-out mechanism from third party information sharing; (2) provide users with

a clear and conspicuous mechanism to set communication, online behavioral advertising, and other preferences that will apply to all covered entities participating in a Choice Program; and (3) establish procedures for testing and review of Choice Program applications, periodic assessment of members, and enforcement for violations by participating entities.[248]While not expressly ***329*** endorsing DNT, the bill does not exclude it as a means to obtain user consent.[249]

2. Commercial Privacy Bill of Rights Act of 2011.

On April 12, 2011, Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the Commercial Privacy Bill of Rights Act of 2011, intended to "establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the FTC."[250]The bill directs the FTC to promulgate rules to require covered entities "to provide clear, concise, timely notice" of their information collection, use, transfer, and storage practices.[251] In addition, a covered entity would be required to provide clear, concise, and timely notice to individuals before changing its practices in a material way.[252] It would not, however, be required to obtain opt-in consent to such changes; rather opt-in consent would only be necessary where a change creates risk of economic or physical harm to an individual.[253]

The bill would require a covered entity "to offer individuals a clear and conspicuous" opt-out mechanism for any "unauthorized use" of covered information, except for any use requiring opt-in consent.[254] "Unauthorized use" is defined as use for any purpose "not authorized by the individual," except certain "commonly accepted" uses by a covered entity or its service provider--including first-party marketing, analytics and ad-tracking-- so long as the covered information used was either collected directly by the covered entity or by its service provider.[255] A "robust, clear, and conspicuous mechanism for opt-out ***330*** consent" must also be provided "for the use by third parties of the individuals' covered information for behavioral advertising or marketing."[256] Opt-in rights must be provided under the bill for collection, use, or transfer of sensitive information--except in limited circumstances--as well as for the use or transfer to a third party of previously collected covered information for an unauthorized use or where there is a material change in the covered entity's stated practices and the use or transfer creates a risk of economic or physical harm to an individual.[257]

The bill directs the FTC to issue rules to establish safe harbor "co-regulatory programs" to be administered by non-governmental organizations.[258] The programs would establish mechanisms for participants to implement the bill's requirements with regard to online behavioral advertising, location-based advertising, and other unauthorized uses.[259] The programs would offer consumers a clear, conspicuous, persistent, and effective means of opting-out of the transfer of covered information by a participant in the safe harbor program to a third ***331*** party.[260]

3. Consumer Privacy Protection Act of 2011.

The Rush bill contains a number of provisions similar to a discussion draft of privacy legislation, which was published by Representatives Rick Boucher (D-VA) and Cliff Stearns (R-FL) in May 2010.[261] On April 13, 2011, Rep. Stearns formally introduced a revised version of the measure, co-sponsored by Rep. Jim Matheson (D-UT),[262] as the Consumer Privacy Protection Act of 2011.[263] The bill would obligate covered entities to provide users with a privacy notice: (1)

before personal information is used for a purpose unrelated to a "transaction,"[264] which is broadly defined to include:

> [A]n interaction between a consumer and a covered entity resulting in any use of information that is necessary to complete the interaction in the course of which information is collected, or to maintain the provisioning of a good or service requested by the consumer, including use . . . related to website analytics methods or measurements for improving or enhancing products or services. . . . [and] the collection or use of personally identifiable information for the marketing or advertising of a covered entity's products or services to its own customers or potential customers . . . .[265]

And "(2) upon any material change in the covered entity's privacy policy."[266] Such a notice would be provided "in a clear and conspicuous manner, be prominently displayed or explicitly stated to the consumer," and state that personal information "may be used or disclosed for purposes or transactions unrelated to that for which it was collected," or "that there has been a material change in the covered entity's privacy policy."[267] In addition, the bill would require covered entities to provide users with a "brief, concise, clear, and conspicuous" privacy policy***332*** statement, "written in plain language."[268]

Under the bill, users must be offered an opportunity to prevent, at no charge for a period of up to five years (unless the user indicates otherwise), the sale or disclosure for consideration of their personal information for a purpose other than the transaction it was collected for.[269] The provision of such an opt-out right is not required if the personal information transferee is an "information-sharing affiliate,"[270] defined as "an affiliate that is under common control with a covered entity, or is contractually obligated to comply with" its privacy policy statement.[271]Realizing that the transfer of personal data often constitutes a primary, not secondary part of the business transaction, the bill permits a covered entity to provide a consumer an opportunity to authorize the sale or disclosure of her personal information "in exchange for a benefit to the consumer."[272] The opportunity offered to consumers to preclude or permit the sale or disclosure for consideration of their personal information "must be both easy to access and use, and the notice of the opportunity to preclude must be clear and conspicuous."[273]

Generally speaking, the Stearns-Matheson bill would solidify the notice and choice paradigm criticized by the FTC and Department of Commerce. Unlike the Kerry-McCain and Rush bills, it does not obligate entities to obtain opt-in consent in any circumstance.

…

Footnotes:

189. Privacy Continues to Dominate the Agenda at Several Agencies and Congressional Committees, Magazine.org (Apr. 8, 2011), http:// www.magazine.org/news/newsletters/washingtonenews/ (follow "MPA Washington Newsletter - April 8, 2011" hyperlink).
190. Privacy, Technology and the Law, U.S. Senate Comm. on Judiciary, http://www.judiciary.senate.gov/about/subcommittees/privacytechnology.cfm (last visited Oct. 7, 2011).

191. See generally Kashmir Hill, Why 'Privacy By Design' is the New Corporate Hotness, Forbes.com (July 27, 2011, 1:23 PM), http:// www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness; Preliminary Report, supra note 155, at v-vii.
192. Preliminary Report, supra note 155, at 53-69.
193. In statements recently made to the Technology Policy Institute's Aspen Forum, FTC Commissioner J. Thomas Rosch recently emphasized transparency, rather than user choice, as the key aspect of DNT. See McCullagh, supra note 16.
194. Christopher Wolf, FTC Proposes Industry-Led 'Do-Not-Track' Mechanism in Long-Awaited Privacy Report, Hogan Lovells (Dec. 2, 2010), http:// www.hldataprotection.com/2010/12/articles/consumer-privacy/bna-article-on-ftc-report-features-hogan-lovells-attorney/.
195. On February 11, 2011, Representative Jackie Speier (D-CA) introduced the Do Not Track Me Online Act of 2011, which would direct the FTC to promulgate DNT regulation for the use of "an online opt-out mechanism to allow a consumer to effectively and easily prohibit the collection or use" of online activity and "to require a covered entity to respect the choice of such consumer to opt-out of such collection or use." Do Not Track Me Online Act, H.R. 654, 112th Cong. § 3(a) (2011). Under the bill, businesses would be required to disclose their information practices to users in an "easily accessible" manner. Id. §3(b)(1). On May 6, 2011, Representatives Ed Markey (D-MA) and Joe Barton (R-TX) introduced the Do Not Track Kids Act of 2011, amending the Children's Online Privacy Protection Act of 1998 (COPPA) to prevent online behavioral tracking of children as well as teens under 18. Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011). On May 9, 2011, Senator Jay Rockefeller (D-WV) introduced the "Do-Not-Track Online Act of 2011," which would instruct the FTC to promulgate regulations that would create standards for the implementation of a DNT mechanism and prohibit online service providers from tracking individuals who use DNT to opt-out. The regulations would allow online service providers to track individuals who opt-out only if tracking is necessary to provide a service requested by the individual and the individuals' information is anonymized or deleted when the service is provided; or the individual is given clear notice about the tracking and affirmatively consents. Do-Not-Track Online Act of 2011, S. 913, 112th Cong. § 2(b) (2011).
196. Preliminary Report, supra note 155, at 66.
197. Id. at 67.
198. Pam Dixon, Consumer Tips: How to Opt-Out of Cookies That Track You, World Privacy F., http://www.worldprivacyforum.org/cookieoptout.html#optout (last visited Oct. 21, 2011).
199. Id.
200. See Sean Harvey & Rajas Moonka, Keep Your Opt-outs, Google Pub. Pol'y Blog (Jan. 24, 2011, 12:00 PM), http:// googlepublicpolicy.blogspot.com/2011/01/keep-your-opt-outs.html.
201. Dixon, supra note 198.
202. Do Not Track Legislation: Is Now the Right Time? Hearing Before the Subcomm. on Commerce, Trade & Consumer Protection of the H. Comm. on Energy & Commerce, 111th Cong. (2010) (statement of David Vladeck, Dir. Bureau of Consumer Protection, Fed. Trade Comm'n).
203. CDT What Does "Do Not Track" Mean?, supra note 7, at 1.
204. Consensus document submitted to the Fed. Trade Comm. by Ari Schwartz, et al., Consumer Rights and Protections in the Behavioral Advertising Sector, at 4 (2007), http://www.worldprivacyforum.org/pdf/ConsumerProtections_ FTC_ConsensusDoc_Final_s.pdf.
205. Id.
206. Jeremy Kirk, Privacy Add-ons Merged to Create Powerful Tool, PCWorld.com (June 15, 2010, 8:20 AM), http:// www.pcworld.com/businesscenter/article/198852/privacy_addons_merged_to_create_ powerful_tool.html; Christopher Soghoian, TACO 2.0 Released, Slight Paranoia (July 27, 2009, 7:00 AM), http://paranoia.dubfire.net/2009/07/taco-20-released.html. See also Christopher Soghoian, The History of the Do Not Track Header, Slight Paranoia (Jan. 21, 2011, 4:00 PM), http:// paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html.

207. Targeted Advertising Cookie Opt-Out (TACO), Mozilla.org, https:// addons.mozilla.org/en-US/firefox/addon/targeted-advertising-cookie-op/ (last visited Oct. 20, 2011); Kirk, supra note 206.
208. Kirk, supra note 206.
209. The History of the Do Not Track Header, supra note 206.
210. Id.
211. See Webcast: Consumer Online Privacy: Hearing Before the Sen. Comm. On Commerce, Sci., & Transp., 111th Cong. (2010) (statement of Jon Leibowitz, Chairman, Fed. Trade Comm'n), http://commerce.senate.gov/public/index.cfm? p=Hearings (browse by July, 2010; then follow "Consumer Online Privacy" link in the results list; then click play button).
212. Compare id., with Consumer Online Privacy: Hearing Before the Sen. Comm. On Commerce, Sci., & Transp., 111th Cong. (2010) (statement of Jon Leibowitz, Chairman, FTC), http:// www.ftc.gov/os/testimony/100727consumerprivacy.pdf.
213. Jonathan Mayer, Ending the Web Privacy Stalemate - DoNotTrack.Us, Stanford.edu (Nov. 15, 2010), http://cyberlaw.stanford.edu/node/6556.
214. Do Not Track: Universal Web Tracking Opt out, http:// donottrack.us/ (last visited Nov. 2, 2011).
215. IAB Reviews Preliminary FTC Staff Report on Protecting Consumer Privacy, Interactive AdvertisingAdver Bureau (Dec. 1, 2010), http:// www.iab.net/public_policy/1481209.
216. Colin O'Malley, Self-Regulation Solves the Do Not Track Problem, Interactive Adver. Bureau (Feb. 23, 2011), http:// www.iab.net/iablog/2011/02/self-regulation-solves-the-do-.html.
217. Id.
218. See Tracking Protection Lists, Microsoft, http:// www.iegallery.com/en/trackingprotectionlists/ (last visited Oct. 31, 2011).
219. See, e.g., Tracking Protection, Microsoft, http:// windows.microsoft.com/en-US/Internet-explorer/products/ie-9/features/tracking-protection (last visited Oct. 31, 2011).
220. IE9 and Privacy: Introducing Tracking Protection, Windows Internet Explorer Engineering BlogWeblog (Dec. 7, 2010, 10:10 AM), http:// blogs.msdn.com/b/ie/archive/2010/12/07/ie9-and-privacy-introducing-tracking-protection-v8.aspx.
221. Id.
222. Microsoft purportedly shelved a similar feature several years ago, under intense pressure from online advertisers. Nick Wingfield & Julia Angwin, Microsoft Adds Privacy Tool, Wall St. J., Mar. 15, 2011, at B1.
223. Id.
224. Aaron Brauer-Rieke, "Do Not Track" Gains Momentum as Mozilla Announces New Tracking Tool, Ctr. Democracy & Tech. (Jan. 24, 2011), http:// www.cdt.org/blogs/aaron-brauer-rieke/%E2%80%9Cdo-not-track%E2%CC80%9D-gains-momentum-mozilla-announces-new-tracking-tool.
225. Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities, Mozilla Blog (Feb. 8, 2011), http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/.
226. Privacy/Jan2011 DoNotTrack FAQ, MozillaWiki, https:// wiki.mozilla.org/Privacy/Jan2011_DoNotTrack_FAQ (last modified Jan. 24, 2011, 9:56 PM).
227. Brauer-Rieke, supra note 224.
228. Harvey supra note 200.
229. Id.
230. Id.
231. Nick Wingfield, Apple Adds Do-Not-Track Tool to New Browser, Wall St. J., Apr. 14, 2011, at B5. For a proposal of implementing DNT through client--as opposed to server-side solutions--see Mikhail Bilenko et al., Targeted, Not Tracked: Client-Side Solutions for Privacy-Friendly Behavioral Advertising, Privacy Enhancing Technologies Symposium (2011), http:// petsymposium.org/2011/papers/hotpets11-final3Bilenko.pdf.
232. For a comparison of proposed mechanisms, see Cooper supra note 93. See also Comments of Jim Brock, Founder & CEO, PrivacyChoice LLC, submitted to the Fed. Trade Comm'n in response to the Preliminary Report (Feb. 18, 2011), available at

http://www.ftc.gov/os/comments/privacyreportframework/index.shtm (follow “PrivacyChoice” hyperlink). The EFF views Mozilla's browser header as the best solution, stating “Mozilla is now taking a clear lead and building a practical way forward for people who want privacy when they browse the web.” Rainey Reitman, Mozilla Leads the Way on Do Not Track, Elec. Frontier Found. (Jan. 24, 2011, 1:16 PM), https://www.eff.org/deeplinks/2011/01/mozilla-leads-the-way-on-do-not-track.
233. Julie Brill, Comm'r, FTC, Address Before the Computer and Communications Industry Association: Privacy and Responsibility 4-5 (May 4, 2011), available at http://www.ftc.gov/speeches/brill/110504ccias.pdf.
234. See supra Part V.A.
235. What They Know, Wall St. J., http:// online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Oct. 7, 2011).
236. See, e.g., Julia Angwin & Amir Efrati, Google Settles with FTC over Google Buzz, Wall St. J. (Mar. 31, 2011), http:// online.wsj.com/article/SB10001424052748703806304576232600483636; Amir Efrati, Google Settles Privacy Lawsuit for $8.5 Million, Wall St. J. (Sept. 3, 2010), http://online.wsj.com/article/SB10001424052748703946504575470510382073.
237. Alasdair Allan & Pete Warden, Got an iPhone or 3G iPad? Apple Is Recording Your Moves, O'Reilly (Apr. 20, 2011), http:// radar.oreilly.com/2011/04/apple-location-tracking.html.
238. In addition to the comprehensive legislation outlined below, two bills were submitted dealing with DNT and one with online behavioral tracking of children. See supra note 195 and accompanying text.
239. Best Practices Act, H.R. 5777, 111th Cong. (2010). On February 10, 2011, Rep. Rush re-introduced the bill in the 112th Congress as H.R. 611. Press Release, Rep. Bobby L. Rush, Rush Introduces Online Privacy Bill, H.R. 611, The Best Practices Act (Feb. 11, 2011), available at http:// www.house.gov/apps/list/press/il01_rush/pr_110211_hr611.shtml.
240. The Best Practices Act, H.R. 611, 112th Cong. §102(a)(2011).
241. Id. §103(a)-(e).
242. Id. §103(f).
243. Id. §§2(8)(A)(VI), 104(b).
244. Id. § 104(a)-(b).
245. Id. § 105(a). The bill also requires covered entities to post new privacy policies that include any such material changes at least 30 days in advance of collecting information pursuant to those policies. Id. § 105(b).
246. Id. § 104(c).
247. Id. § 401.
248. Id. §§ 403-404.
249. Upon re-introduction of his bill in the 112th Congress, Representative Rush said, “I do not oppose Do-Not-Track. In fact, in order for companies to qualify under the FTC Safe Harbor program contained in my bill, they would have to set up a ‘Do-Not-Track like’ mechanism for consumers to allow them to opt-out of having the personal information they provide, both online and offline, to third parties.” Press Release, supra note 239.
250. Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011); Commercial Privacy Bill of Rights, Senate.gov, http:// kerry.senate.gov/work/issues/issue/?id=74638d00-002c-4f5e-97091cb51c6759e6&CFID=74356785&CFTOKEN=59186701 (last visited Oct. 20, 2011).
251. Commercial Privacy Bill of Rights Act, S. 799, 112th Cong. §201(a)(1) (2011).
252. Id. § 201(a)(2).
253. Id. § 202(a)(3)(B).
254. Id. § 202(a)(1).
255. Id. § 3(8). In the context of online behavioral tracking, it is worth noting the following exceptions from the definition of “unauthorized use” (meaning that the following activities do not require opt-out rights): “To market or advertise to an individual from a covered entity within the context of a covered entity's own Internet website, services, or products if the covered information used for such marketing or advertising was--(I) collected directly by the covered entity; or (II) shared with the covered entity--(aa) at

the affirmative request of the individual; or (bb) by an entity with which the individual has an established business relationship." Id. § 3(8)(B)(vi). "Use that is necessary for the improvement of transaction or service delivery through research, testing, analysis, and development." Id. § 3(8)(B)(vii). "Use that is necessary for internal operations, including the following: ... Information collected by an Internet website about the visits to such website and the click-through rates at such website--(aa) to improve website navigation and performance; or (bb) to understand and improve a the interaction of an individual with the advertising of a covered entity." Id. § 3(8)(B)(viii)(II). "Use--(I) by a covered entity with which an individual has an established business relationship; (II) which the individual could have reasonably expected, at the time such relationship was established, was related to a service provided pursuant to such relationship; and (III) which does not constitute a material change in use or practice from what could have reasonably been expected." Id. § 3(8)(B)(ix).
256. Id. § 202(a)(2). A "third party" is defined as a person that is not related to the covered entity by common ownership or control; is not the covered entity's service provider; does not have an "established business relationship" with the individual; and does not identify itself to the individual at the time of information collection. Id. § 3(7). The term "established business relationship" means a relationship formed with or without consideration, involving the establishment of an account for the receipt of products or services. Id. §3(4).
257. Id. § 202(a)(3).
258. Id. § 501.
259. Id. § 501(a).
260. Id. § 501(a)(2).
261. Rick Boucher, A Bill to Require Notice to and Consent of an Individual Prior to the Collection and Disclosure of Certain Personal Information Relating to that Individual (May 3, 2010) (discussion draft), available at http:// www.nciss.org/legislation/BoucherStearnsprivacydiscussiondraft.pdf.
262. Rick Boucher failed to get re-elected in the 2010 mid-term elections. Tony Romm, Tech Community Laments Rick Boucher Loss, Politico (Nov. 2, 2010), http://www.politico.com/news/stories/1110/44589.html.
263. Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Cong. (2011).
264. Id. § 4(a)(1).
265. Id. § 3(14)
266. Id. § 4(a)(2).
267. Id. § 4(b).
268. Id. § 5(a)-(b).
269. Id. § 6(a).
270. Id.
271. Id. 3(7).
272. Id. § 6(b).
273. Id.§ 6(c).

Behavioral Advertising: From One-Sided Chicken to Informational Norms

Richard Warner & Robert H. Sloan
Vanderbilt Journal of Entertainment and Technology Law
Volume: 15
Beginning on page: 49
Fall, 2012

[51]

You download the free audio recording software from Audacity. [1] Your transaction is like any traditional provision of a product for free or for a fee, with one difference: you agree that Audacity may collect your information and use it to send you advertisements. [2] Billions of such pay-with-data exchanges occur daily. [3] They feed information to a complex advertising ecosystem that constructs individual profiles for "behavioral advertising." [4] Behavioral advertising is "the tracking of consumers' online activities [52] in order to deliver tailored advertising." [5] It merges our digital footprints into pictures of surprising intrusiveness and accuracy. Advertisers can determine where you work, how and with whom you spend your time, and "with 87% certainty … where you'll be next Thursday at 5:35 p.m." [6] The consequence is a startling loss of informational privacy. Informational "privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [7] Others now have considerable power to collect, analyze, and use our information. [8] We - most of us - want considerably more control over our information than the advertising ecosystem allows. [9] But we also want the advantages information processing secures: increased availability of relevant information, increased economic efficiency, improved security, and personalization of services. [10] We [53] are willing to trade some privacy for some of the advantages, but we want a better trade-off than the control-depriving one businesses currently impose on us. Our misgivings are evidently idle, however. We routinely enter pay-with-data exchanges when we visit CNN.com, use Gmail, or visit any of a vast number of other websites. [11] Why? And, what should we do about it?

We answer both questions by describing pay-with-data exchanges as a game of Chicken that we play repeatedly under conditions that guarantee that we will always lose. Chicken is traditionally played with cars. [12] Two drivers speed toward each other; the first to swerve loses. We play a similar game with sellers, with one crucial difference: we know in advance that the sellers will never "swerve." We will call this game "One-Sided Chicken."

How do we escape One-Sided Chicken and regain an appropriate degree of control over our information? Regaining control means ensuring ourselves a sufficiently broad ability to give free and informed consent to information processing; otherwise, we lack sufficient ability to determine - by and for ourselves - what information others collect about us, and how they use and distribute it. Currently, businesses purport to obtain consent through "Notice and Choice."[13] The "notice" is the presentation of information [54] (typically in a privacy policy and terms-of-use agreement), while the "choice" is a consumer action (typically using the site, or clicking on an "I agree" button), which is interpreted as the choice to proceed under the presented

terms. [14] As we have argued elsewhere and will assume here, "notice and choice" is clearly inadequate. [15] It does not ensure informed consent: people do not read and acquire the information necessary to make informed choices. [16] Moreover, it cannot ensure informed consent; as Daniel Solove and others have emphasized, you need information about unpredictable future uses of your data to make an informed choice, and you cannot know what you cannot know. [17] Even if it were possible, and even if people made the effort to be informed, notice and choice should not be the mechanism we use. There is no reason to think that the combined result of the individual choices would yield the socially optimal trade-off between privacy and the goals served by collecting information. [18]

The key to achieving free and informed consent lies instead in informational norms. [19] Informational norms are social norms that constrain the collection, use, and distribution of personal information. [20] Such norms explain, for example, why your pharmacist may inquire about the drugs you are taking but not about whether you are happy in your marriage. Norm-governed exchanges not only implement acceptable trade-offs between informational privacy and competing goals, but they also ensure that we give free and informed consent to those trade-offs. [21] Unfortunately, rapid advances in information-processing technology have greatly outpaced the relatively slow evolution of norms, and lacking norms, we lack any adequate way to give free and informed consent to acceptable privacy trade-offs. The right response is to create the necessary norms, and we will suggest an appropriate norm-generation process.

…

I. The Online Advertising Ecosystem

We present a simplified model of the advertising ecosystem consisting of just five entities: profilers, advertising agencies, advertising networks or exchanges, websites that display the advertisements, and businesses that purchase the advertisements. [32] A single entity may perform more than one role, but we may ignore that complication for the purposes of this model.

A. A Simple Ecosystem Model

Profilers create profiles that segment buyers into groups in order to predict their willingness to buy specific types of products and services. [33] eXelate, for example, has agreements with hundreds of websites that allow it to collect information about age, sex, ethnicity, marital status, profession, Internet search information, and information about sites visited. [34] It combines this data with data from offline sources. [35] eXelate explains,

> We are capturing billions of deep granular data points … . We analyze [these data points] … and roll them into specific Targeting Segments … . These categorizations include Demographic data … , consumer Interest data gathered from specific site [58] activity … (such as parenting and auto enthusiast sites), and deep purchase Intent data culled from relevant … activity on top transactional sites. We further segment and sub-segment this data into relevant buckets that in many cases drill down to the product and keyword level. [36]

Profiles routinely identify particular individuals, despite frequent claims to the contrary from practitioners of behavioral advertising. [37] TARGUSinfo, for example, boasts that "with our authoritative data and proprietary linking logic, no other company can match our ability to accurately identify businesses and consumers in real time - helping you target and recognize your best prospects, even at the moment of live interaction." [38] The data includes "names, addresses, landline phone numbers, mobile phone numbers, email addresses, IP addresses and predictive attributes." [39] The purpose of the profiles is to target display advertising. [40] A business may create its own display advertising, or it may outsource that to an advertising agency. [41]

Advertising exchanges and networks, such as Google's AdSense, deliver display advertisements to the websites that display them. [42] When a buyer visits a website, an advertising exchange combines the buyer's profile with information about his or her current website activity in order to more precisely target advertisements. [43] The exchange then conducts an auction in which businesses bid for the opportunity to present their targeted advertisements (the whole process takes milliseconds). [44] As one commentator aptly sums up the situation, "Advertisers bid against each other in real time for the ability to direct a message at a single Web surfer." [45] The goal is to [59] tailor advertisements as closely as possible to the interests of the buyer receiving them. [46] Datran Media, for example, promises "to identify who is visiting your Web site, who is being exposed to your advertisers' campaigns, and who is responding to specific ads. Real-time reports paint an accurate picture of whom your audience really is and who is responding to your communications - at the household level!" [47] The amount of information processed is immense. Right Media Exchange processes 9 billion advertising purchases daily; [48] MediaMath, 13 billion daily; [49] TARGUSinfo, 62 billion a year; [50] and Pubmatic, one hundred thousand per second. [51] The number of Google's AdSense transactions is not available, but it is a network of 1.5 million websites and advertisers. [52] Participation in AdSense is free for the seller and a route into the advertising ecosystem for small businesses and free giveaways like Audacity. [53]

Widespread participation in the advertising ecosystem makes it quite difficult for buyers to find websites that will conform to their privacy preferences. The lack of buyer choice plays a key role in our characterization of pay-with-data exchanges as a game of One-Sided Chicken.

B. Buyers' Lack of Choice

Buyers lack choice because, although advertising is personalized, information processing is not. Information processing does not vary to conform to the privacy preferences of individual buyers. Efficient information processing requires standardized, automated routines using supercomputing power and advanced statistical techniques to analyze vast collections of a complex mix of [60] data from a variety of online and offline sources. [54] Marketing objectives - not buyers' privacy preferences - drive the collection, analysis, and use of vast amounts of diverse types of information. [55] As the CEO of the advertising exchange Rocket Fuel notes, the company's "technology drives results for advertisers by automatically leveraging massive amounts of internal and third-party external data and serving only the best impressions in the context of each advertiser's unique marketing objectives." [56]

Sellers do not tailor their information processing to buyers' privacy preferences because they do not need to. As we explain in detail in the next section, the vast majority of buyers acquiesce in

information-processing practices, thereby guaranteeing sellers significant advertising revenues. Thus, sellers can easily afford to ignore the relatively few buyers who refuse to do business with them unless they adjust their information-processing practices. [57] But even so, shouldn't we expect some sellers to break the mold to win business by catering to privacy preferences? That expectation would be disappointed. [58] Sellers do not break the mold - not if they rely on advertising as a significant source of revenue. [59] Participation in the ecosystem gives a seller a competitive edge over nonparticipants by [61] making it a more attractive advertising platform. [60] To compete, other sellers must also participate, and, to gain an edge, they may need to adopt even more privacy-invasive practices. The result is a "race to the bottom." [61]

…

The first step is to introduce and explain norms.

III. Norms, Coordination Norms, Informational Norms

We define norms in general first and then turn to the special case of coordination norms. Finally, we focus on the type of coordination norm that concerns us here: informational norms.[71]

A. Norms Generally

We define norms in terms of nearly complete conformity. A "norm" is a behavioral regularity in a group, where the regularity exists at least in part because almost everyone thinks that he ought to conform to the regularity. [72] We leave open the question of how many [66] must conform for almost everyone in a particular group to conform, as well as the question of how to define the group within which conformity occurs ("almost everyone" means "almost everyone in such-and-such group"). An example: In Jones's small town, everyone goes to a Protestant church on Sunday. They do so at least in part because each believes he or she ought to go.

B. Coordination Norms

Our primary concern is with coordination norms. A coordination norm is a behavioral regularity in a group, where the regularity exists at least in part because almost everyone thinks that, in order to realize a shared interest, she ought to conform to the regularity, as long as everyone else does. [73] The key difference from the Protestant church example is that there is a shared interest people can realize only through coordinated action. This is not true of the church example: people can attend church even if others do not. Driving on the right is a classic example. In the United States and other "drive on the right" countries, we drive on the right because, and only as long as, almost everyone else does so. [74] No one would drive on the right if she expected everybody else to drive on the left. Which side of the road one drives on depends on where one expects others to drive. However, everyone thinks that, for safety and convenience, all [67] drivers should drive on the same side. One cannot achieve this goal alone; one needs the cooperation of others.

Similarly, in elevator etiquette, the norm is to maximize the distance to your nearest neighbor.[75] The norm balances two competing interests: using the elevator when it arrives, and

avoiding overcrowding. All share an interest in being able to use the elevator and avoiding overcrowding, and no one can realize the interest unilaterally. We think we ought to conform to achieve this balance - as long as everyone else does so. There is little point in being a "nearest-neighbor distance maximizer" if everyone else just stands wherever they like.

In both examples, everyone conforms to the regularity (driving on the right, maximizing distance from the nearest neighbor) because everyone thinks that, to realize the shared interest, he or she ought to conform, as long as everyone else does. We define coordination norms with reference to this "shared interest/ought to conform, as long as everyone else does" pattern. The "ought" is conditioned on the assumption about everyone else. We will need to refer to such "oughts" frequently, and, to avoid constant repetitions of "as long as everyone else does," we will say, for short, that one thinks one ought conditionally to conform. [76]

We focus on the role of coordination norms in mass markets. In mass markets, coordination norms shape buyers' demands. A mass-market buyer cannot unilaterally ensure that sellers will conform to his or her requirements; coordination norms create collective demands to which profit-motive-driven sellers respond. One key question: Who are the parties subject to demand-unifying norms in mass markets? The answer may at first seem obvious: buyers and sellers. After all, they need to coordinate so that sellers supply what buyers demand; and, if the norms are to allocate risks between buyers and sellers, how could both not be parties to the norm? However, while it is possible to model mass-market demand-unifying norms as [68] buyer-seller coordination norms, [77] it is simpler and more elegant to model them as norms to which the only parties are buyers. The key point is that producers design and sell mass-market products in response to sufficiently large groups of buyers. Hence, no mass-market buyer can unilaterally ensure, for example, that his desired level of privacy will be available; only a sufficiently large collective demand can accomplish that. Coordination via demand-unifying norms creates the required collective demand, to which profit-motive-driven sellers respond. Since the profit motive is sufficient to ensure that sellers respond, there is no need to see the sellers as a party to the coordination norm. Demand-unifying norms take the following form: "buyers demand that sellers … ." The reference to sellers may suggest, contrary to what we said earlier, that both buyers and sellers are parties to the norm. This is a misimpression. Buyers are the only parties subject to the norm. The norm coordinates their demands, and sellers respond - not because they are parties to the norm, but because they want to profit by meeting the unified demand. [78]

C. Informational Norms

The informational norms with which we are concerned are coordination norms that govern the collection, use, and distribution of information. [79] As Helen Nissenbaum notes, informational norms generally … circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed. In medical contexts, it is appropriate to share details of our physical condition or, more specifically, the patient shares information about his or her physical condition with the physician but not vice versa; among friends we may pour over romantic entanglements (our own and those of others); to the bank or our creditors, we reveal financial information; with our professors, we discuss our own grades; at work, it is appropriate to discuss work-related goals and the details and quality of performance. [80]

In commercial contexts, informational norms are generally instances of the following pattern: buyers demand that the seller collect, use, and distribute information only as is appropriate for that [69] seller's role. [81] The shared interest is that businesses confine themselves to role-appropriate processing. [82] Relying on the work of Nissenbaum and others, we assume that transactions between consumers and businesses occur against a background of informational norms. [83] An example is in order, however.

Imagine Vicki is shopping in a wine store. The relevant norm is that the store may process information only in ways appropriately related to the store's role as a retailer of wine. This norm strikes a balance between privacy and the ends served by information processing by only permitting the processing of some information and only for certain purposes. Vicki cannot implement this balance on her own. A mass-market buyer cannot unilaterally ensure that sellers will conform to the buyer's requirements; coordination norms create collective demands to which profit-motive-driven sellers respond. [84] Informational norms - like coordination norms generally - play a key role in mass markets by unifying buyers' demands to the point that mass-market sellers will meet those demands. [85] For example, it is currently a norm that buyers demand personal computers with a [70] graphical interface. [86] However, if almost all buyers demanded a UNIX command line interface, mass-market sellers would meet that demand and ignore the few buyers that want a graphical interface. [87]

D. Value-Optimal Norms

A cornerstone of our analysis is that coordination norms - and hence informational norms - may or may not be value-optimal. A coordination norm is value-optimal when, in light of the values of all (or almost all) members of the group in which the norm obtains, the norm is at least as well justified as any alternative. [88] A norm that is at least as well justified as any alternative is either better justified than any alternative or is tied with one or more alternatives that are also better than the rest. This is why it is appropriate to call a norm "value-optimal" when it is at least as well justified as any alternative: there is no better alternative. [89] There are many optimality notions; Pareto optimality is perhaps the most well known. [90] Value-optimality is the notion for our purposes. A terminological point: In the informational-privacy context, we will broaden our use of "value-optimal" to apply both to informational norms and to trade-offs between privacy and competing goals. A trade-off is value-optimal when it is at least as well justified as any alternative.

As we argue below, when value-optimal informational norms govern mass-market transactions, buyers give free and informed consent to acceptable trade-offs between informational privacy and competing concerns. [91] The concern here is that, in a number of important cases, rapid advances in information-processing technology have outstripped the relatively slow evolution of norms and created novel situations for which we lack relevant value-optimal [71] informational norms. There are two ways in which value-optimal norms may be lacking: (1) relevant norms exist, but they are not value-optimal; or (2) relevant norms do not exist at all. The consequence is the same in each situation: we lack any effective mechanism to give free and informed consent. Instead, we submit to poor trade-offs between privacy and competing goals. Behavioral advertising is an instance of the second type of case; they lack the relevant norms altogether. We

have discussed the "norms but not value-optimal" cases in detail elsewhere. [92]

Before we turn to the lack of norms for behavioral advertising, it is important to understand what buyers are missing when the transactions they enter are not governed by value-optimal norms. Accordingly, we first explain how value-optimal informational norms ensure free and informed consent to acceptable trade-offs.

E. Norms and Consent

We need to answer three questions about exchanges governed by value-optimal informational norms: (1) Why are the trade-offs the norms implement acceptable to buyers? (2) In what sense is consent to the trade-offs "informed"? And, (3) in what sense is consent "free"? The first question is easy to answer. Information processing consistent with a value-optimal norm implements a trade-off that is acceptable in the sense that it is justified by buyers' values, and there is no alternative that is better justified. The answer to the second question requires a bit more elaboration.

A natural first response is that informed consent requires awareness of the ways in which the information will be used. This will not do, however. Current information-processing practices store data for very long times for later use in ways that are unpredictable at the time a buyer consents to the data collection. [93] Therefore, the buyer's consent cannot be informed if being informed means being [72] aware of how the data will be used. The options are either to conclude that consent cannot be informed or to seek another understanding of what it means for consent to be informed. We choose the latter course. We will regard consent as informed provided the buyer knows that the consent is to practices governed by a value-optimal norm. To know that the practices are governed by a value-optimal norm is to know that norm-consistent uses of the buyer's information - both uses now and uses, whatever they may be, in the unpredictable future - will implement trade-offs between privacy and competing goals that are, in light of the buyer's values, at least as well justified as any alternative.

Explaining why consent counts as free is more problematic than explaining why it counts as informed. Consider Vicki. As a practical matter, she cannot avoid consenting to the norm-imposed trade-off. Of course, she could simply not buy wine at all, but she enjoys wine and is not willing to give it up, nor is she willing to spend time and effort investigating the exact information-processing practices of the local wine stores. She is already committed to a variety of goals - raising her children, pursuing her career, enjoying her friends, and so on - and the time she is willing to allot to buying wine is relatively brief. Acquiescing to norm-permitted information processing is her only viable option. So how can her consent be free?

Are constrained choices after all the example par excellence of unfree choices? When a thief, with a gun to your head, demands, "Your money or your life!" the thief violates your freedom by compelling your choice. The only meaningful option is to hand over your money. There is no gun to the head in informational-norm-governed transactions, but options are, in practice, typically reduced to one - conform to the norm. Does the lack of options not entail a lack of freedom?

The answer lies in the fact that even a highly constrained choice can still be a free choice. Imagine, for example, that you have your heart set on a vacation in the Cayman Islands; unfortunately, your tight budget appears to make the trip impossible. Your solution is to constrain your choices by opting for an "all inclusive" vacation package that offers airfare, hotel, and food for a single affordable price. In doing so, you voluntarily constrain your food options in order to freely realize your vacation goal, and, when you eat the hotel food, you do so as an essential means to realizing your vacation goal and hence as something fully justified in light of your values. Your constrained choice is free in the sense that it is a fully justified component of a freely chosen overall plan. Contrast the thief example. Giving the money to the thief is not a fully justified part of your overall plan; it is an unjustified interference with it.

[73] Similar analysis holds for Vicki's wine-store transaction. She allots only a relatively small amount of time to purchasing wine. She wants to purchase suitable wine within that time and return to pursuing her other goals. She knows the store will process some range of personal information, and she wants an acceptable trade-off between her informational privacy and the various interests served by processing the information. The wine-store norm - processing personal information only in ways appropriately related to the store's role as a seller of wine - offers her a ready-made trade-off, and, as long as the norm is value-optimal, the trade-off is not only justified in light of her values, but there is also no alternative that is better justified.

We conclude that, when buyers conform to value-optimal norms, buyers give free and informed consent to the norm-implemented trade-offs. When we take value-optimal norms away from mass-market buyer/seller exchanges, we lose the background that ensures free and informed consent to acceptable trade-offs. The problem that concerns us is that relevant value-optimal coordination norms do not exist for pay-with-data exchanges. We first argue that the norms do not exist, and we then turn to explaining how to create the necessary value-optimal norms.

F. Lack of Norms for Pay-With-Data Exchanges

The argument that pay-with-data exchanges lack norms turns on the definition of coordination norms as regularities to which the parties to the norm coordinate to realize a shared interest.[94] The shared interest in the case of informational norms is that sellers limit themselves to role-appropriate information processing.[95] We claim that relevant informational norms do not exist for pay-with-data exchanges because we lack widely shared notions of role-appropriate information processing for such exchanges. An analogy shows why.

Suppose that, unbeknownst to each other, two long-time friends have become expert chess players. When they begin to play friendly games together, they at first have no norms that govern how they will use their chess-playing powers against each other. How should they deal with victory and defeat? Should the victor be reassuring or taunting? In a losing position, how long should one struggle hoping for an error before acknowledging defeat and resigning? They lack shared conceptions of role-appropriate behavior as chess players. As they play, those conceptions and the associated [74] coordination norms develop, but they do not exist at first. They arise over time out of repeated interactions.

We are in a similar situation with pay-with-data exchanges. The newly acquired power is the

vastly increased ability to process information, and we lack relevant shared conceptions of role-appropriateness. These conceptions will only evolve over time through patterns of social and commercial interaction. Instead of shared conceptions of appropriateness, we have the intense controversy that surrounds behavioral advertising today. As we noted earlier, buyers are willing to trade some privacy for some of the advantages of permitting extensive information processing, but buyers want a better trade-off than the one the advertising ecosystem currently imposes on them. [96] Any adequate response to behavioral advertising must strike the proper balance, and as James Rule notes, "We cannot hope to answer [complex balancing questions] until we have a way of ascribing weights to the things being balanced. And that is exactly where parties to privacy debates are most dramatically at odds." [97] We lack shared conceptions of role-appropriate information processing in many cases, but in particular in pay-with-data exchanges.

…

V. Norm Creation in Real Markets

…

A. A Norm-Generation Process

Our solution assumes that every buyer possesses close-to-perfect "do not track" technologies. A tracking-prevention technology would be perfect if it were completely effective in blocking information processing for advertising purposes, completely [79] transparent in its effect, effortless to use, and it permitted a user full use of any website.

We begin with a summary of our proposed norm-generation process: (1) buyers will use the "do not track" technologies; (2) use of these technologies will threaten sellers with a dramatic decline in advertising revenue; (3) sellers will respond by offering buyers information processing consistent with their preferences; and (4) the ultimate result will be a collection of value-optimal norms governing pay-with-data transactions.

1. Buyers Will Use the Technologies

As we noted at the beginning, the vast majority of buyers wants greater control over their information than current information-processing practices allow. We assume that the desire for control is sufficiently strong that buyers would block tracking if they had close-to-perfect tracking-prevention technologies. If this turns out not to be true, it would certainly be necessary to reevaluate the surveys that report buyers' strong objections to current behavioral advertising. [111]

2. Advertising Revenue Will Decline

The result of buyers using close-to-perfect do-not-track technologies used is a loss of advertising revenue for sellers. Sellers' advertising revenue is a function of the number of advertisements on their websites and the number of responses to them. [112] The attractiveness of a website as an advertising platform depends on the effectiveness of advertisements on that website. [113] In the online advertising ecosystem, this effectiveness is a function of the amount and accuracy of the information collected from the site about buyers. [114] When all buyers block the collection of such

information, the effectiveness of advertisements declines, and websites lose a good [80] deal of their attractiveness as advertising platforms. [115] Advertisers are more likely to spend their advertising budgets elsewhere - on TV, radio, and print-publication advertisements. Thus, it does not matter that advertisers are a significant source of revenue. Websites lose that revenue when they lose their attractiveness as advertising platforms.

3. Sellers Will Conform More Closely to Buyers' Preferences

Sellers will respond by offering information processing consistent with buyers' preferences. They will, that is, if they can segment buyers into groups of shared preferences, and if at least some of the groups are sufficiently large that the expected profit from meeting those groups' preferences is greater than the cost of not doing so. We fully expect buyers to cluster into such groups. Even if they do not initially, sellers will be able to form such groups of buyers through advertising. Advertising can powerfully shape buyers' demands. Direct-to-consumer advertising of prescription drugs is an excellent example; it has increased the demand for such drugs. [116] Website use is similar. Accessing websites for all sorts of purposes is now such an entrenched feature of daily life that not doing so is no longer an option. Accessing websites has a "side effect," however - the collection and commercialization of information about buyers. Advertising that promotes trade-offs between the benefits and the "side effect" should coalesce buyer demand more or less as well as prescription-drug advertising. So sellers will conform to buyers' preferences by shaping those preferences in ways that make conformity profitable. Like Phoebe when she sees Tony in the car, sellers will "swerve" to avoid losing the advertising revenue that they "love."

We contend that a collection of norms will arise as a result. This final conclusion, contemplating whether those norms are truly value-optimal, merits a separate subsection.

B. Norms? Yes. Value-Optimal? Yes, But …

The result of the process outlined above will be a number of behavioral regularities of the form, "buyers demand such-and-such trade-off." Eventually, not only will the trade-offs be value-optimal, but buyers will also believe they are. Recall that consumers are currently not even close to consensus about how to strike a [81] value-optimal trade-off between privacy and the benefits of information processing. As advertising unites buyer demand into suitably sized groups, buyers will continue to engage in billions of pay-with-data exchanges daily. Over time, the trade-offs implemented in the exchanges will cease to be merely accepted; they will become acceptable. Buyers will ultimately recognize the trade-offs as value-optimal. Buyers' values will have evolved and transformed so that they regard the trade-offs as at least as well justified as any alternative. At that point, the regularities will be coordination norms. Buyers will conform to the regularity because we think we ought to (our values dictate that we ought), and the "ought" will be conditional. A buyer thinks she ought to conform only as long as almost all others do; if almost all others demanded some other trade-off, the buyer would think she ought conditionally to do so, too. Sellers would not meet an idiosyncratic demand, so, as long as foregoing the services is not an acceptable option, the buyer will think she ought to demand the trade-off conditionally. [117]

So is this not what was wanted? A way out of One-Sided Chicken that yields value-optimal norms? That depends. We (the authors) have no doubt that the process will lead to value-optimal norms, but will it be a process that as a society we will later regret? What one values in one's youth, as a result of a personality-shaping factor, one may regret when one is older. The same may happen society-wide. It is possible, for example, that the process leads to the world Daniel Solove dreads, the world in which a permanent, ever-growing, readily searchable trail of information records the trivial to the intimate to the unfortunate details of our lives from childhood onward. [118] How can we avoid such regrettable outcomes?

Our suggestion is to rely on consumer educational initiatives.[119] They can powerfully shape buyers' preferences. For example, the spread of health information has led, over the last twenty years, to a per capita increase in poultry consumption at the expense of beef consumption. [120] The explanation presumably is that education altered [82] the values about health and enjoyment that guide people's food choices. [121] Our hope is that consumer education will direct value formation away from regrettable paths.

…

Footnotes:

1. Audacity: Free Audio Editor and Recorder, http:// audacity.sourceforge.net (last visited Sept. 6, 2012).
2. Privacy Policy, Audacity, http:// audacity.sourceforge.net/contact/privacy (last visited Sept. 6, 2012).
3. See Tania Karas, 10 Things Online Data Collectors Won't Say, SmartMoney.com (Apr. 5, 2012, 12:34 PM), http:// www.smartmoney.com/spend/technology/10-things-online-data-collectors-wont-say-1333598586287.
4. See Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814, 1852-53 (2011).
5. Fed. Trade Comm'n, FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising 2 (2009), http:// www.ftc.gov/os/2009/02/P085400behavadreport.pdf [hereinafter FTC Staff Report].
6. Lucas Mearian, Big Data to Drive a Surveillance Society, Computerworld (Mar. 24, 2011, 1:23 PM), http:// www.computerworld.com/s/article/9215033/Big_data_to_drive_a_surveillance_ society.
7. Alan F. Westin, Privacy and Freedom 7 (1967) (emphasis added).
8. We do not distinguish between personally identifying information (PII) and non-PII, because recent advances in de-anonymization ensure that, in many cases, non-PII may in fact identify individuals. See, e.g., Arvind Narayanan & Vitaly Shmatikov, Robust De-anonymization of Large Sparse Datasets, 2008 IEEE Symposium on Security and Privacy 111 (2008); Schwartz & Solove, supra note 4, at 1814.
9. This is the most plausible interpretation of over twenty years of studies and surveys about consumer attitudes toward privacy. For an excellent collection of relevant studies, see The Economics of Privacy, Carnegie Mellon Univ., http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm (last visited Sept. 6, 2012). For a useful summary of consumer attitudes in this regard, see Joshua Gomez et al., Know Privacy, Univ. Cal. Berkley, Sch. of Info. (June 1, 2009), http://knowprivacy.org/report/KnowPrivacy_Final_Report.pdf. For discussion and interpretation, see Richard Warner, Undermined Norms: The Corrosive Effect of Information Processing Technology on Informational Privacy, 55 St. Louis U. L.J. 1047-48 (2011) [hereinafter Undermined Norms].
10. For a discussion of the advantages (other than personalization of services), see Jerry Kang, Information Privacy in Cyberspace Transactions, 50 Stan. L. Rev. 1193 (1998) (emphasizing availability of relevant information, increased economic efficiency, and improved security). For a discussion of consumer willingness to trade privacy for various benefits, see Karl W. Lendenmann, Consumer

Perspectives on Online Advertising--2010, PreferenceCentral 3 (2010), http:// www.preferencecentral.com/consumersurvey/download ("Over half of consumers surveyed indicated that they prefer relevant targeted online ads as a trade-off for access to free content."), and ChoiceStream, Inc., 2006 ChoiceStream Personalization Survey, http://www.choicestream.com/pdf/ChoiceStream_ PersonalizationSurveyResults2006.pdf (last visited Sept. 7, 2012) (claiming that only 15 percent of web users would give up personalization benefits to avoid revealing personal details). But see Joseph Turow et al., Americans Reject Tailored Advertising and Three Activities that Enable It (Soc. Sci. Research Network, Working Paper, 2009), available at http:// ssrn.com/abstract=1478214 (arguing that the vast majority of consumers find behavioral advertising unacceptable). The opposing studies illustrate the well-known truth about surveys: what you ask determines what you get. Still, the most reasonable interpretation of the surveys is that consumers (more or less) reject the current privacy/efficiency trade-off and want a trade-off that gives them more control over their privacy.

11. See, e.g., Wendy Schuchart, Google Privacy Policy Changes? Get Over It, IT Knowledge Exchange (Jan. 27, 2012, 2:22 PM), http:// itknowledgeexchange.techtarget.com/cio/google-privacy-policy-changes-get-over-it ("Facebook basically knows enough about me to successfully predict what I'm going to wear tomorrow, yet we all grudgingly accept Zuckerberg's evil empire and go on with our status updates.").

12. The 1955 film classic, Rebel Without a Cause, popularized the game of Chicken. In the film, Jim Stark (James Dean) races Buzz toward a cliff edge; the first to jump out loses. Rebel Without a Cause (Warner Bros. Pictures 1955). Bertrand Russell popularized the "drive toward each other" version when he described the mid-twentieth century nuclear brinksmanship policies of the United States and the Soviet Union as a game of Chicken. See Bertrand Russell, Common Sense and Nuclear Warfare 29-31 (1959). There is a very readable discussion of the game of chicken in William Poundstone, Prisoner's Dilemma 197-201 (1992). Chicken, also known as Hawk-Dove, is a standard game-theory game. See, e.g., Kevin Leyton-Brown & Yoav Shoham, Essentials of Game Theory: A Concise, Multidisciplinary Introduction 29, 80 (2008); Martin J. Osborne & Ariel Rubinstein, A Course in Game Theory 16-17 (1994).

13. For a description and criticism of Notice and Choice, see Comments of The Center for Digital Democracy & U.S. PIRG, In re A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Feb. 18, 2011), http:// www.ftc.gov/os/comments/privacyreportframework/00338-57839.pdf [hereinafter Center for Digital Democracy Comments]. See also J. Howard Beales III & Timothy J. Muris, Choice or Consequences: Protecting Privacy in Commercial Information, 75 U. Chi. L. Rev. 109, 112-14 (2008); Paul M. Schwartz, Internet Privacy and the State, 32 Conn. L. Rev. 815, 822-23 (2000); cf. Paul Ohm, The Rise and Fall of Invasive ISP Surveillance, 2009 U. Ill. L. Rev. 1417, 1496 (endorsing a limited notice-and-choice regime).

14. See Schwartz, supra note 13, at 824 ("[W]hen a Web site says something about its data processing practices--even if this statement is vague or reveals poor practice--the visitor to the site is deemed to be in agreement with these practices so long as she sticks around. This summary, despite its ironic tone, is no exaggeration.").

15. See Richard Warner & Robert Sloan, The Undermining Impact of Information Processing on Informational Privacy, in Rights of Personality in the XXI Century (Justyna Balcarczyk ed., 2012) [hereinafter The Undermining Impact of Information Processing]; Richard Warner & Robert Sloan, Unauthorized Access: The Crisis in Online Privacy and Information Security (forthcoming 2012) [hereinafter Unauthorized Access].

16. Beales & Muris, supra note 13, at 135.

17. Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stan. L. Rev. 1393, 1452 (2001).

18. See The Undermining Impact of Information Processing, supra note 15; Unauthorized Access, supra note 15.

19. See infra Part III.C.

20. See infra Part III.C.

21. See infra Part III.E.

…
32. Models may distinguish several more entities and functions. For example, some make a subtle distinction between advertising networks and advertising exchanges. See, e.g., Data Usage & Control Primer: Best Practices & Definitions, Interactive Adver. Bureau 12 (2010), http:// www.iab.net/media/file/data-primer-final.pdf.
33. See Mark MacCarthy, New Directions in Privacy: Disclosure, Unfairness and Externalities, 6 I/S: J.L. & Pol'y for Info. Soc'y 425, 462-64 (2011).
34. See Emily Steel, Exploring Ways to Build a Better Consumer Profile, Wall St. J., Mar. 15, 2010, http:// online.wsj.com/article/SB10001424052748703447104575117972284656.
35. See id.
36. Rev Share and Rental Pricing Models Bring Accountability to eXelate Data Exchange Says CEO Zohar, AdExchanger (May 28, 2009, 7:20 AM), http:// www.adexchanger.com/data-exchanges/data-exchange-exelate-zohar.
37. See Center for Digital Democracy Comments, supra note 13, at 15-20.
38. TARGUSinfo, On-Demand Scoring, http:// www.targusinfo.com/solutions/scoring/on-demand-scoring (last visited Sept. 8, 2012).
39. TARGUSinfo, Our Data: Not All Data Is Created Equal, http:// www.targusinfo.com/about/data (last visited Sept. 8, 2012).
40. See Dustin D. Berger, Balancing Consumer Privacy with Behavioral Targeting, 27 Santa Clara Computer & High Tech. L.J. 3, 4 (2011) (“These profiles allow websites and ISPs to serve advertisements and other services that are targeted to their customers' interests.”).
41. For examples of advertising agencies, see Epsilon, Strategy & Analytics, http://www.epsilon.com/analytic-focused-services; Havas Media, Our Group, http://www.havasmedia.com/our-group; Omnicom Group, National Advertising Agencies, http://www.omnicomgroup.com/ourcompanies/nationaladvertisingagencies.
42. See AdSense Basics, Google, http:// support.google.com/adsense/bin/answer.py?hl=en&answer=9712 (last visited Sept. 21, 2012).
43. See Schwartz & Solove, supra note 4, at 1851-52.
44. See id. at 1852.
45. Garett Sloane, amNY Special Report: New York City's 10 Hottest Tech Startups, amNY (Jan. 25, 2010), http://www.amny.com/urbanite-1.812039/amny-special-report-new-york-city-s-10-hottest-tech-startups-1.1724369.
46. See Aperture: Audience Measurement, Datran Media, http:// web.archive.org/web/20100222080259/http:// www.datranmedia.com/aperture/audience-measurement/index.php?showtype=for-publishers (last visited Sept. 12, 2012).
47. Id.
48. Complaint, Request for Investigation, Injunction and Other Relief at 2, In re Real-time Targeting and Auctioning, Data Profiling Optimization, and Economic Loss to Consumers and Privacy, F.T.C. (Apr. 8, 2010), available at http://www.centerfordigitaldemocracy.org/sites/default/files/20100407-FTCfiling.pdf.
49. Id.
50. Id.
51. Id.
52. Helen Leggatt, Google Discloses Size of Its Ad Network, BizReport (May 26, 2010), http://www.bizreport.com/2010/05/google-discloses-size-of-its-ad-network.html.
53. AdSense Revenue: Do I Have to Pay to Use AdSense?, Google, http:// support.google.com/adsense/bin/answer.py?hl=en&answer=32850 (last visited Sept. 24, 2012).
54. See, e.g., Rocket Fuel CEO John Says Ad Exchanges More Like a Technology Platform than Media Source, AdExchanger (Aug. 24, 2009, 6:07 AM), http://www.adexchanger.com/ad-networks/rocket-fuel-ad-exchanges.
55. See id. (describing marketing objectives but not mentioning buyers' privacy preferences).
56. Id. (emphasis added).

57. One study may suggest the opposite. See Sören Preibusch & Joseph Bonneau, The Privacy Landscape: Product Differentiation on Data Collection (The Tenth Workshop on the Econ. of Info. Sec., Working Paper, 2011), available at http://weis2011.econinfosec.org/papers/The%20privacy%C20landscape%20-%20Product%20differentiation%C20on%C20data%c̈ol.pdf. The study shows that when buyers can detect differences in the privacy characteristics of goods and services, sellers offering roughly homogeneous goods and services try to differentiate themselves by catering to privacy preferences. Id. at 3. There is no inconsistency with our claims, however. The study considered only the amount of personal information requested for registration (if any) in mandatory or optional fields and whether the website had a privacy policy. Id. at 5. The study did not "include technical data collected implicitly such as a users' IP address or stored third-party cookies." Id. Since such information is critical for behavioral advertising, we cannot infer from the study that websites would differentiate with regard to such data (even if visitors were able to detect whether the website collected it).
58. See Felicia Williams, Internet Privacy Policies: A Composite Index for Measuring Compliance to the Fair Information Principles, F.T.C. (2006), http://www.ftc.gov/os/comments/behavioraladvertising/071010feliciawilliams.pdf ("The vast majority of the privacy policies stated the firms have the right to share any data with any third party for any reason.").
59. Not all sellers do. Dropbox's revenue model, for example, relies on user fees for data storage to generate revenue. See 10 Revenue Models for Social Media Startups, STARTUPFREAK (Aug. 30, 2012), http:// www.startupfreak.com/10-revenue-models-for-social-media-startups.
60. A Race to the Bottom: Privacy Ranking of Internet Service Companies, Privacy Int'l (June 9, 2007), http://www.privacyinternational.org/reports/a-race-to-the-bottom-privacy-ranking-of-internet-service-companies/a-consultation-report-0.
61. Id.
…
71. We discuss these matters in detail in Unauthorized Access, supra note 15. There are earlier discussions in Richard Warner & Robert H. Sloan, Vulnerable Software: Product-Risk Norms and the Problem of Unauthorized Access, 2012 U. Ill. J.L. Tech. & Pol'y 45; The Undermining Impact of Information Processing, supra note 15. In the text we offer a brief summary.
72. Our notion of a norm is a standard one in recent law and economics literature, with one exception. We explain conformity to the norm by appeal to people's beliefs above what they ought to do. The recent literature in contrast explains conformity as the result of self-interested actors avoiding the costs of nonconformity. "[One] approach typically assumes that people care only about their own (material) well being, and rely on repeated game models to explain how they cooperate or refrain from violating social norms.... [A] second approach typically assumes that people care about something else aside from material goods--esteem, or status, or conformity, or some such thing." Eric A. Posner, Introduction to Social Norms, Nonlegal Sanctions, and the Law xi-xii (Eric A. Posner ed., 2007). Richard McAdams, a proponent of the second approach, notes that "by norm I mean a decentralized behavioral standard that individuals feel obligated to follow, and generally do follow ... [to gain the esteem of others], or because the obligation is internalized, or both." Richard H. McAdams, The Origin, Development, and Regulation of Norms, in Social Norms, Nonlegal Sanctions, and the Law 101, 144 (Eric A. Posner ed., 2007). The emphasis on "feeling obligated" would appear close to our view that people conform because they think they ought to; however, McAdams explains "feeling obligated" in terms of the costs of non-conformity--thus: "Without internalization, one obeys the norm to avoid external sanctions.... After internalization, there is yet another cost to violating a norm: guilt. The individual feels psychological discomfort whether or not others detect her violation." Id. McAdams still conceives of people as self-interested agents seeking to avoid costs they regard as unacceptable. We take it to be clear that people are not merely self-interested agents. The assumption that they are has been extensively and decisively criticized. See, e.g., Amartya Sen, The Idea of Justice 32-33 (2009).
73. See Undermined Norms, supra note 9, at 1060.

74. H. Peyton Young, The Economics of Convention, 10 J. Econ. Persp. 105, 107-08 (1996) (providing a game-theoretic explanation of the decision made by individual drivers as to whether to drive on the right or left side of the road).
75. This is a simplification. The true norm is closer to "maximize the distance from your nearest neighbor subject to the constraint that you stay within the peripheral vision of at least one other passenger, and that you have at least one other passenger within your peripheral vision." See generally Where we stand in an elevator, You the User (Apr. 26 2012), http:// youtheuser.com/2012/04/26/where-we-stand-in-an-elevator.
76. Our notion shares similarities with the notion proposed in Steven A. Hetcher, Norms in a Wired World (2004). There are also important affinities between our notion of a coordination norm and the notion of a coordination game. The original idea of coordination games and the term "coordination game" comes from David K. Lewis, Convention: A Philosophical Study (1969); Lewis's notion of a convention, in turn, is inspired by Thomas C. Schelling, The Strategy of Conflict (1960). For a more recent treatment, see Russell W. Cooper, Coordination Games: Complementarities and Macroeconomics (1999).
77. But see supra text accompanying note 60.
78. Helen Nissenbaum, Privacy as Contextual Integrity, 79 Wash. L. Rev. 119, 120-21 (2004).
79. Not all informational norms are coordination norms. For example, our norm-generation process under conditions of perfect competition produces an informational norm that is not a coordination norm. See infra Part IV.B. It is only in real markets that the process produces a coordination norm. See infra Part V.B. However, since real markets are our ultimate concern, the informational norms that primarily concern us are coordination norms.
80. Nissenbaum, supra note 78, at 138.
81. "Role-appropriateness" is determined contextually. Over a wide range of cases, group members share a complex set of values that leads them to more or less agree in their particular contextual judgments of appropriateness. "Within each context, the relevant agents, the types of information, and transmissions principles combine to shape the governing informational norms." Michael Zimmer, Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine, 3 J. Bus. & Tech. L. 109, 115 (2008). Norms vary from group to group. For simplicity, however, we take the relevant group to be all US consumers.
82. This interest in sticking to role-appropriate processing is shared only among buyers, not buyers and sellers; as we emphasized earlier, our mass-market coordination norms are buyer-only norms. See supra Part III.B. This is one reason to choose a buyers-only approach to modeling mass-market coordination norms. We could still model the norms as having buyers and sellers as parties and make the point about buyers sharing an interest in only role-appropriate information processing, but the price would be considerable complication.
83. For a small sample of this diverse literature, see Pierre Bourdieu & Loïc J.D. Wacquant, An Invitation to Reflexive Sociology (1992); Michael Philips, Between Universalism and Skepticism: Ethics as Social Artifact (1994); Michael Walzer, Spheres Of Justice: A Defense of Pluralism and Equality (1983); Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 Stan. L. Rev. 1373 (2000); Roger Friedland & Robert R. Alford, Bringing Society Back In: Symbols, Practices, and Institutional Contradictions, in The New Institutionalism in Organizational Analysis 232 (Walter W. Powell & Paul J. DiMaggio eds., 1991); Helen Nissenbaum, Protecting Privacy in an Information Age: The Problem of Privacy in Public, 17 Law & Phil. 559 (1998); James Rachels, Why Privacy is Important, 4 Phil. & Pub. Aff. 323 (1975); Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609 (1999); Jeroen van den Hoven, Privacy and the Varieties of Informational Wrongdoing, in Readings in Cyber Ethics 430 (Richard A. Spinello & Herman T. Tavani eds., 2001).
84. See supra note 78 and accompanying text.
85. See supra notes 86-91 and accompanying text; infra notes 86-100 and accompanying text.
86. See Jeremy Reimer, A History of the GUI, Ars Technica (May 5, 2005, 1:40 AM), http://arstechnica.com/features/2005/05/gui ("It is pretty much assumed whenever anyone sits down to use a personal computer that it will operate with a graphical user interface. We expect to interact with it

primarily using a mouse, launch programs by clicking on icons, and manipulate various windows on the screen using graphical controls. But this was not always the case.").
87. See supra text accompanying notes 84-98.
88. To avoid misunderstanding, we should note that we are not, for example, saying that when you step into an elevator, you explicitly think about where you ought to stand. Typically, people just unreflectively conform to the norm. The point is that you could justify conformity if you reflected on the norm under ideal conditions (including having sufficient time, sufficient information, lack of bias, and so on).
89. See supra note 88 and accompanying text; infra notes 90-104 and accompanying text.
90. A situation is Pareto optimal when, and only when, it is not possible to improve the well-being of any one person without making others worse off.
91. See infra Part III.E-F.
92. An example of a norm that is not value-optimal is the "no helmet" norm among pre-1979 National Hockey League players. Thomas C. Schelling, Hockey Helmets, Concealed Weapons, and Daylight Saving: A Study of Binary Choices with Externalities, 17 J. Conflict Resol. 381, 381 (1973). In 1979, the League mandated wearing helmets. Id. Prior to that time, not wearing a helmet was a behavioral regularity that existed in part because each player thought he ought to conform, as long as all the others did--primarily to appear tough, and secondarily to have slightly better peripheral vision. Id. However, because of the value they placed on avoiding head injuries, virtually all the players regarded the alternative in which they all wore helmets as better justified. Id. However, they remained trapped in the suboptimal norm. Id. We argued elsewhere that the same happens with informational privacy. Id. Our most recent and complete argument is in Unauthorized Access, supra note 15. An earlier, shorter argument is in Undermining Impact of Information Processing, supra note 15.
93. See Solove, supra note 17.
94. See supra Part III.B.
95. See supra Part III.B.
96. See supra notes 6-7 and accompanying text.
97. James B. Rule, Privacy in Peril 183 (2007).
…
111. See supra note 10.
112. See Omer Tene, Privacy: The New Generations, 1 Int'l Data Privacy L. 15, 16-17 (2010), available at http:// idpl.oxfordjournals.org/content/1/1/15.full; see also AdWords Help: Cost-per-click Bidding, Google, http://support.google.com/adwords/bin/answer.py? hl=en&answer=2459326 (last updated Sept. 17, 2012) (discussing the per-click, per-view, and per-conversion advertisement-bidding processes for the placement of ads on Google's search result pages, blogs, and ad network).
113. See Tene, supra note 112, at 16-17.
114. See Omer Tene & Jules Polonetsky, To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising, 13 Minn. J. L. Sci. & Tech. 281, 283; FTC Staff Report, supra note 5, at 2; Tene, supra note 112, at 16-17.
115. Cf. Ira S. Rubinstein, Regulating Privacy by Design, 26 Berkeley Tech. L.J. 1409, 1440 (2011).
116. Meredith B. Rosenthal et al., Demand Effects of Recent Changes in Prescription Drug Promotion, 6 Frontiers Health Pol'y Res. 1 (2003).
117. Buyers may divide into several groups each with a different opinion about what trade-off is value-optimal. As long as the groups are large enough (and sellers can identify who belongs to which group), different coordination norms may arise for each group.
118. Daniel J. Solove, The Future of Reputation: Gossip, Rumor, and Privacy on the Internet 17 (2007).
119. The Federal Trade Commission's efforts illustrate the type of educational initiatives we have in mind. Since the rise of e-commerce in 1995, "the Commission has conducted a series of public workshops and has issued reports focusing on online data collection practices, industry's self-regulatory efforts, and technological efforts to enhance consumer privacy." FTC Staff Report, supra note 5.
120. Henry W. Kinnucan et al., Effects of Health Information and Generic Advertising on U.S. Meat Demand, 79 Am. J. Agric. Econ. 13 (1997).

121. See id. at 20 (“That health concerns may play an important role in explaining meat consumption patterns is suggested by the magnitude of the estimated health information elasticities of ... poultry and ... beef[, which] hint at the potential importance of health information in explaining increases in poultry consumption and declines in beef consumption over time.”).

New Directions in Privacy: Disclosure, Unfairness and Externalities

Mark MacCarthy
I/S: A Journal of Law and Policy for the Information Society
Volume: 6
Starting Page: 425
Summer, 2011

**426* I. Introduction

Privacy policy is back. Policymakers and the public are again concerned about the collection of personal information by businesses and its possible misuse. The Federal Trade Commission has released a report re-conceptualizing privacy policy.[2] The Department of Commerce issued its own privacy report,[3] and it is co-chairing an interagency working group on privacy.[4] Legislation regulating online privacy has been introduced in the U.S. House of Representatives.[5] The European Commission announced a re-examination of its Data Protection Directive to see if parts of it need to be upgraded in light of new economic and technological developments.[6] The International Conference of Privacy and Data Protection Commissioners drafted a new international privacy standard.[7]

But what is the best way to protect privacy? Many of the revived concerns raised by privacy advocates and political leaders focus on the lack of control by data subjects over the collection and use of their ****427*** personal information, and they propose policies to increase individual control over the collection and use of information.[8]

This Article argues that this informed consent model of privacy regulation is deeply flawed. I rehearse some traditional criticisms of this model and then draw attention to the difficulties that negative privacy externalities create for the informed consent approach. The second major contribution of this Article is to describe a more promising alternative regulatory approach.[9] The unfairness model of privacy regulation described in this Article would allow policymakers to evaluate directly the outcomes of information use without focusing solely on creating an ideal information collection process.

In the United States, the "informed consent" model[10] has endured because it is based on two compelling ideas: (1) that privacy has to do with the ability of data subjects to control information about them, and (2) that people have very different privacy preferences.[11] In principle, informed consent allows data subjects to control information according to their own preferences.

****428*** Despite this intuitive appeal, the informed consent model has been widely criticized.[12] Internet privacy policies and the federally mandated financial privacy notices are often cited as examples of the failure of this approach. They are largely unread, not very informative, and written too broadly. They would also be astonishingly costly to read. In 2009, researchers at Carnegie Mellon estimated that the cost to the economy of the time spent reading Internet privacy notices would be $781 billion per year.[13]

As many have pointed out, the problems are more fundamental than how to get notices read. Restrictions on disclosure are impractical in a digital world where information collection is ubiquitous, where apparently anonymous or de-identified information can be associated with a specific person, and where data analytics on large or linked databases can allow extraordinary and unpredictable inferences.[14] It is no longer reasonable to expect a typical Internet user to understand what information is collected about him or her online, what can be inferred from that information, and what can be done with the profiles and analytics based on that information. In this context, relying on informed consent to prevent information harms would be similar to letting people decide for themselves what level of exposure to toxic substances they would accept in the workshop or the environment.

I add to these standard criticisms of the informed consent model by focusing on negative privacy externalities, where one person's decision to share information can adversely affect others who choose ***429*** to remain silent. The idea is that disclosure of information by some people can reveal information about other people, to their detriment. A striking example is the revelation of people's sexual orientation through an analysis of their social network friends.[15] Another example is the unraveling of privacy protections in the context of eligibility decisions, where those with a favored characteristic have an incentive to disclose, thereby outing those who remain silent. Non-smokers are happy to tell insurance companies about their healthy habits, thereby identifying the smokers. These contexts and the use of data analytics to discover information about people other than the data subject are pervasive and likely to grow more common as the power of data analytics increases.

While the idea that data analytics can reveal previously hidden information about a data subject has been treated in the literature extensively,[16] there has not been sufficient attention paid to the idea that certain contexts of information disclosure and data analytics can reveal information about people other than the data subject.[17] This external effect undermines the normative appeal of the informed consent model. It is no longer only the data subject's interest that is at stake in information disclosure, but the interests of other people who are not parties to the transaction. A focus on privacy externalities also provides some explanation of why people seem to care about the privacy decisions that others make.[18]

The notion of a negative privacy externality does not rely on intangible non-quantifiable feelings of privacy violations, and it allows the conceptualization of privacy as inherently social. Under this conception, privacy concerns can express reservations about an indefinitely large class of possible economic harms that the mere refusal to disclose would not avoid. Even when individuals have the ***430*** ability to refuse data collection requests, if enough other people go along with the information collection and use scheme, the economic damage is done.

An unfairness framework for privacy needs to supplement the informed consent model. If the harm done by negative privacy externalities is substantial, then individual choice might have to be restricted. Simply getting informed consent would not make an information practice legitimate. One way to structure an unfairness framework is by dividing the collection and use of information into three categories. Impermissible collection and use of information is so harmful that even with data subject consent it should not be permitted. Public benefit use of information

is so important that it should be allowed even without data subject consent. In between lies the realm of consent, where information can be collected and used subject to an opt-in or opt-out regime. An opt-in regime would make sense for the information uses that are closer to the impermissible uses and opt-out would be adopted for the information uses closer to the public benefit use. In effect, unfairness acts as a floor, blocking some information uses from reaching the level of individual choice.

…

II. The Limitations on Informed Consent

A. Premises of the Informed Consent Model

The informed consent model can be summed up in two propositions: informed consent is necessary to obtain legitimacy and it is sufficient to obtain legitimacy. With informed consent, any information collection and use practice is legitimate. Without it, no information collection and use practice is legitimate. There might be other rules relating to the fair use of information, but the heart of the informed consent model is this intimate connection between legitimacy and consent.[21]

…

B. General Criticisms of the Informed Consent Model

One line of criticism of the informed consent model is that it is expensive and impractical. The financial privacy notices that were required by federal legislation following the passage of the Gramm-Leach-Bliley Act's privacy requirements illustrate the weakness of the disclosure approach.[24] Billions of dollars were spent designing, testing, and mailing annual privacy notices that almost no one reads and that are virtually incomprehensible if read; the total cost has been estimated at between $2 and $5 billion per year.[25] In 2001, the trade association America's Community Banks estimated that the "average compliance cost was $1.37 per customer, with total estimated compliance costs per bank ranging widely from as little as $1,000 to more than $2 million."[26] No one's privacy is furthered by these empty requirements for formal notification. If the goal was to induce people to opt out of certain information sharing practices, it has failed. Fewer than 5% of those receiving notices chose to opt out of third-party information sharing.[27]The condemnation of the approach is from both privacy advocates[28] and critics of the idea of privacy rights.[29]

***436** Privacy policies on the Internet are equally unread. As of 2002, Yahoo reported that less than 1% of its visitors read its privacy policy.[30] Google's recent attempt to provide more granular privacy notices and its ability to control how visitors are categorized has attracted tens of thousands of people per week, but that is a "tiny fraction of the user base of the world's largest search engine."[31] This is a good thing. These policies are also virtually incomprehensible and astonishingly costly to read. Researchers at Carnegie Mellon concluded that if all U.S. consumers read all the privacy policies for all the websites they visited just once a year, the total

amount of time spent on just reading the policies would be 53.8 billion hours per year and the cost to the economy of the time spent doing this would be $781 billion per year.[32]

Additional objections to the informed consent model based on the practicalities of informing people and obtaining their consent are well taken. For example, how is consent for secondary use supposed to be obtained without using the very information that is at issue?[33]

The development and growth of data collection, aggregation and analytics over the last decade also make informed consent impractical. It no longer seems reasonable to expect people to fully understand how information about them can flow, how it can be analyzed and how ***437** it can be used to adversely affect their own interests.[34] Fully informed consent to protect the release of information about a data subject is no longer a reasonable goal.

…

E. Negative Privacy Externalities

1. Concept of Negative Privacy Externalities

People have privacy interests that can be adversely affected even when they do not reveal information about themselves and when others do not reveal information about them either. For instance, if a person does not reveal his sexual orientation, but his Facebook friends do, his sexual orientation is thereby revealed.[58] In one study, a person did not say anything about his sexual orientation; neither did his friends. His sexual orientation was revealed to external observers, however, who put together separate pieces of information and analyzed them.[59]Similar inferences about people, in the absence of self-revelation or explicit revelation by others, can be made in a wide variety of circumstances. This Section explores the privacy harms that can result from these information leakages.

Privacy harms of this kind are negative privacy externalities. They are not a separate kind of harm in addition to physical, financial and other tangible harms that can occur to individuals.Negative privacy externalities are these individual harms that are imposed upon individuals by privacy choices made by others.[60]

Privacy externalities are composite. They consist of an information externality together with an evaluation of that externality as harmful. The first step in understanding negative privacy externalities is to understand how data collectors, aggregators, and analysts can infer information about individuals, even when these individuals do not reveal that information themselves, when others do not divulge it ***446** either, and when it is not specifically recorded in public or private databases to which they have access. This leakage might be described as an information externality. Many commentators and privacy scholars have pointed out the ways that information about the data subject can be combined with other information and linked to supposedly anonymous databases. Without realizing it, individuals can expose vast quantities of information about themselves, simply because they do not know what can be done with the information about themselves that they do reveal.[61]

…

***474* B. The Unfairness Framework**

Instead of a framework that relies on notice and choice alone, the unfairness framework creates several categories of information collection and use and varies the regulatory response depending on the category. At one extreme lie those practices involving the collection and use of information that are impermissible even with data subject choice. Call them harmful or impermissible uses of information. At the other extreme stand those practices involving the collection and use of information that are so important that they should be allowed even without data subject choice. Call them public benefit uses. In between lies the realm of choice.

One way to measure the value of the information use is expected social utility, defined as the net social gain or loss discounted by the probability of it occurring. This way of thinking about benefits and harms obviously fits most closely with the economic framework of cost-benefit analysis, which normally involves a quantitative comparison of costs and benefits. But quantification and measurement have to be relative to the type of benefit and harm involved. In many cases, the type of harm involved such as an affront to human dignity or the benefit to human welfare derived from an increase in autonomy and opportunity will be real effects of an information practice that are not amenable to expression in quantitative terms. A qualitative assessment might be all that is possible in many cases.[133]

The focus is social, not individual. The fact that some individuals or groups of individuals benefit or are harmed by an information practice does not automatically mean that it is a social gain or a social loss. The perspective is on what is on balance good for society as a whole. Equity gains or losses have to be taken into account as well to the extent that policymakers reach the judgment that harms or gains to specific groups are worthy of special consideration.

Finally, the perspective has to be probabilistic. Existing information practices can be evaluated in part by their actual consequences. But even then an assessment has to be made of the likely evolution of the information practice in the future and how an industry might adjust to any perceived harms. New innovative uses of information have no track record and so the assessment would have to be based on the likely results of adding the new practice to the existing ***475*** mix of information practices and contexts. The level of uncertainty in these evaluations has to be taken into account when considering any regulatory regime.

The unfairness regime does not ignore the role of informed consent. But it treats informed consent as one regulatory tool among others. Within the unfairness framework, the first step is the provision of information so that consent can be informed. Providing information to consumers can be done in one of two ways: disclosure and notification. Disclosure is the public acknowledgement of an information collection and use practice.[134] Notification is the provision of this information to a specific individual.[135]

Notice and opt-out would be an appropriate policy response when the information practice in question is closer to the public benefit use. Notice and opt-in would be the appropriate policy when the information practice is riskier, closer to the harmful uses. Easy opt-in choice is

especially problematic when an information practice has substantial external information effects that spread the harmful effects beyond those who have chosen to participate in it.

Footnotes:

2. Fed. Trade Comm'n, Protecting Consumer Privacy in an Era of Rapid Change, December 2010, available at http:// www.ftc.gov/os/2010/12/101201privacyreport.pdf, (last visited March 14, 2011).
3. Dep't of Commerce, Notice of Inquiry, Information Privacy and Innovation in the Internet Economy, 75 Fed. Reg. 21,226 (Apr. 23, 2010) [hereinafter Commerce Privacy NOI], available at http:// www.gpo.gov/fdsys/pkg/FR-2010-04-23/pdf/2010-9450.pdf.
4. Subcomm. on Privacy & Internet Pol'y, Comm. on Tech., Nat'l Sci. & Tech. Council, Charter, available at http://www.privacylives.com/wp-content/uploads/2010/11/102010-nstc-privacy-subcommittee-charter.pdf.
5. Rick Boucher, Press Release, U.S. Congressman, Boucher, Stearns Release Discussion Draft of Privacy Legislation, May 3, 2010. The initial reaction was not favorable from either privacy advocates or industry representatives. See Proposed Privacy Legislation Wins Few Fans, Wall St. J., May 4, 2010, http://blogs.wsj.com/digits/2010/05/04/proposed-privacy-legislation-wins-few-fans/tab/print.
6. European Comm'n, A Comprehensive Approach on Personal Data Protection in the European Union, Nov. 4, 2010, available at http:// ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.
7. Int'l Conference of Data Prot. and Privacy Comm'rs, International Standards on the Protection of Personal Data and Privacy, Nov. 5, 2009, available at http://www.privacyconference2009.org/dpas_space/space_ reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_ en.pdf.
8. In releasing his draft privacy legislation, Representative Boucher said, “Our legislation confers privacy rights on individuals, informing them of the personal information that is collected and shared about them and giving them greater control over the collection, use and sharing of that information.” See Boucher, Press Release, supra note 5.
9. Policymakers might be falling back on notice and consent for lack of an alternative. See FTC, Exploring Privacy: A Roundtable Series (Dec. 7, 2009) (introductory remarks of FTC Chairman Jon Leibowitz), available at http:// www.ftc.gov/speeches/leibowitz/091207privacyremarks.pdf (“We do feel that the approaches we've tried so far-both the notice-and-choice regime, and later the harm-based approach-haven't worked quite as well as we would like. But it could be that this issue is a lot like Churchill's view of democracy: ‘it has been said that democracy is the worst form of government except all those other forms that have been tried from time to time.”’).
10. It is the basic structure for the Children's Online Privacy Protection Act of 1998, 15 U.S.C.§§ 6501-06 (2006), the FTC's privacy principles, see FTC, Fair Information Practice Principles, available at http:// www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited March 14, 2011), and the financial privacy provisions in Title V of the Gramm-Leach-Bliley Act of 1999, 15-U.S.C. §§6801-09 (2006). I call it the informed consent model rather than the notice-and-choice (or notice-and-consent) model because this label directly states its enormous normative appeal. People can be said to express their approval of a social practice if they fully understand it and willingly engage in it. A social practice seems to be legitimate when individuals have so consented to it.
11. In their modern incarnations, both ideas derive from Alan Westin. Alan F. Westin, Privacy and Freedom (Atheneum, 1968) (1967).
12. See Fred H. Cate, The Failure of Fair Information Practice Principles, in Consumer Prot. In The Age Of The Info. Econ. (Jane K. Winn ed., 2006); Daniel J. Weitzner, et al., Information Accountability, (Computer Sci. & Artificial Intelligence Laboratory Technical Report MIT-CSAIL-TR-2007-034, 2007), available at http://dspace.mit.edu/bitstream/handle/1721.1/37600/MIT-CSAIL-TR-2007-034.pdf.

13. Aleecia McDonald & Laurie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J.L & Pol'y for Info. Soc'y 543, (2008) available at http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.
14. The Department of Commerce summed up these criticisms as follows: "[T]he customary notice-and-choice approach to consumer protection may be outdated, especially in the context of information-intensive, Web-based services . . . [O]nline interactions and web-based information linkages have become so complicated that it is increasingly difficult to provide consumers truly meaningful notice-and-choice." Commerce Privacy NOI at 21,229, available at http://www.gpo.gov/fdsys/pkg/FR-2010-04-23/pdf/2010-9450.pdf; see also James Nehf, Recognizing the Societal Value in-Information Privacy, 78 Wash. L. Rev. 1, 66 (2003). (After surveying the difficulties in individual-level policing of privacy he concluded: "More 'notice and consent' requirements are not likely to provide greater privacy protection.").
15. See Matthew Moore, Gay Men 'Can Be Identified by Their Facebook Friends', The Telegraph, Sept. 21, 2009, http:// www.telegraph.co.uk/technology/facebook/6213590/Gay-men-can-be-identified-by-their-Facebook-friends.html.
16. See, e.g., Paul Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA L. Rev. 1701 (2009).
17. One exception is T.Z. Zarsky, Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society, 56 Me. L. Rev. 13, 42-46 (2004).
18. See Luc Wathieu, Marketing and Privacy Concerns, (Harvard Business School Working Paper, 2006), for an assessment of these "indirect privacy concerns." available at: http://citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1.106.4252&rep=rep1&type=pdf.
…
21. The original fair information practices developed by the U.S. Department of Health, Education and Welfare (HEW) express this idea of informed consent. Three of the five HEW principles focus on knowledge of data collection and use are: 1. there must be no personal data record keeping systems whose very existence is secret, 2. there must be a way for an individual to find out what information about him is in a record and how it is used, 3.there must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent. U.S. Dept. of Health, Educ., & Welfare, Report of the Sec'y's Advisory Comm. on Automated Personal Data Sys., Records, Computer, and the Rights of Citizens vii (1973), available at http:// aspe.hhs.gov/datacncl/1977privacy/toc.htm. It is also contained in the 1980 OECD guidelines. See OECD, Guidelines on the Prot. of Privacy and Transborder Flows of Pers. Data, Oct. 1, 1980. The collection limitation, use limitation and openness principles all seem to require consent. OECD, Privacy Guidelines, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html. The 1995 European Union Data Protection Directive contains it as well. See Council Directive 95/46/EC, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 95 [hereinafter European Data Protection Directive]. The purpose limitation and transparency principles relate to knowledge and consent.
…
24. Cate, supra note 12, at 365.
25. Id. (noting that financial privacy notices cost an estimated $2-5 billion).
26. 27An Examination of The Gramm-Leach-Bliley Act Five Years After Its Passage 27 before the S. Comm. on Banking, Housing and Urban Affairs, 108th Cong. 43 (2004) (prepared statement of Harry P. Doherty, Vice Chairman of the Board, Independence Cmty. Bank Corp).
27. Cate, supra note 12, at 361.
28. See Tena Friery & Beth Givens, 2001: The GLB Odyssey-We're Not There Yet: How Consumers Rial Privacy Notices and Recommendations for Improving Them, (Dec. 4, 2001) (unpublished comments from Get Noticed: Effective Financial Privacy Notices, FTC public workshop),available at http:// www.privacyrights.org/ar/fp-glb-ftc.htm (describing the financial privacy notices as "a costly experiment that resulted in little effective education of the public about the rights to privacy of personal financial information under GLB").

29. See Timothy Muris, Chairman, FTC, Remarks at the Privacy 2001 Conference, Protecting Consumers' Privacy: 2002 and Beyond, (Oct. 4, 2001) (stating that “acres of trees died to produce a blizzard of barely comprehensible privacy notices.”).
30. Cate, supra note 12, at 361.
31. See Dan Perry, Google Executive Pushes Privacy Concerns, ABCNews.com, Oct. 26, 2010, http://abcnews.go.com/Technology/wireStory? id=11975665. Google's chief privacy officer, Peter Fleisher, is quoted as saying he is “puzzled” about why more people don't use the dashboard's privacy controls.
32. McDonald & Cranor, supra, note 13, at 17. The authors do not treat their study as an argument against notice-and-choice, but as an indication that privacy has to be made easier to understand.
33. As Cate notes, “[M]ost mailing lists are obtained from third parties. For a secondary user to have to contact every person individually to obtain consent to use the names and addresses on the list would cause delay, require additional contacts with consumers, and almost certainly prove prohibitively expensive. And it could not be done without using the very information that the secondary user is seeking consent to use. Cate, supra note 12, at 362. This article also details the difficulties for telephone companies to obtain consent to analyze calling patterns to offer them new services, id. at 361, the difficulties of credit card companies in reaching consumers to ask consent to assess their eligibility for credit offers, id. at 364, and the difficulties of charities in reaching out to their potential donors, id. at 365.
34. See Weitzner et al., supra, note 12, at 1. Lundblad and Masiello make a similar point: “According to some, online interactions and web-based information linkages have become so complicated that it is increasingly difficult to provide consumers truly meaningful notice-and-choice.” Nicklas Lundblad & Betsy Masiello, Opt-in Dystopias, 7 SCRIPTed 155 (2010), available at http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.asp. Other studies demonstrate the ease with which people can be identified from supposedly anonymous data sets. See, e.g., Latanya Sweeney, Uniqueness of Simple Demographics in the U.S. Population (Lab. for Int'l Data Privacy, Working Paper No. LIDAP-WP4 (2000) (arguing that 87.1% of the U.S. population can be identified by their zip code, date of birth and gender); Ohm, supra, note 16. The Wall Street Journal's series on “What They Know” investigated the various ways in which online entities are able to find out information about you. See, e.g., Justin Scheck, Stalkers Exploit Cell Phone GPS, Wall St. J., Aug. 2, 2010 available at http://online.wsj.com/article/SB10001424052748703467304575383522318244?mod=WS J_article_RecentColumns_WhatTheyKnow. Browser settings are another way in which people can be identified by websites they visit. See Erik Larson, Browser Fingerprints: A Big Privacy Threat, PC World, Mar. 27, 2010, available at http://www.networkworld.com/news/2010/032710-browser-fingerprints-a-big-privacy.html. The Electronic Frontier Foundation has a test to determine how unique your browser settings are. When I took the test in August 2010, I had a browser fingerprint that was unique among the 1,126,161 visitors tested up until that point. The EFF test can be taken at https://panopticlick.eff.org/index.php?action=log&js=yes. The Wall Street Journal also reports that companies like [x 1] have technology that enables websites to identify crucial characteristics of their visitors including in one case that that a visitor was “a young Colorado Springs parent who lives on about $50,000 a year, shops at Wal-Mart and rents kids' videos.” Emily Steel & Julia Angwan, On the Web's Cutting Edge, Anonymity in Name Only, Wall St, J., Aug. 4, 2010, available at http://online.wsj.com/article/SB10001424052748703294904575385532109190?mod=WS J_article_RecentColumns_WhatTheyKnow. While not revealing the name of website visitors, enough accurate information was revealed so as to enable credit card companies to target their offers. Id.
…
58. See Moore, supra note 15.
59. Id.
60. For a good general account of externalities see Richard Cornes & Todd Sandler, The Theory of Externalities, Public Goods and Club Goods 3-25 (Cambridge University Press 1996) (1986). In this way, privacy externalities differ from the harm to social goods emphasized by Allen and Regan.

61. One striking example of this is the willingness of people to reveal answers to common security questions on their social network pages. See Americans Exposing Answers to Common Security Questions and Identities on Social Networks, ID Analytics, Nov. 9, 2010, http://www.idanalytics.com/news-and-events/news-releases/2010/11-5-2010.php..
…
133. See Ohm, supra note 16, at 29 (“Before enacting any privacy law, lawmakers should weigh the benefits of unfettered information flow against its costs and must calibrate new laws to impose burdens only when they outweigh the harms the laws help avoid.”).
134. Disclosure can be accomplished by a public description of the information collected and how it is used. Privacy policies posted on an internet site are one example. They are made available to all and apply equally to all.
135. Individualized notice is the transmission to customers of detailed information about a company's collection and use of information. Each customer must receive a separate notification. GLBA financial privacy notices are examples as are the individual notices sometimes required under data breach notification laws. Individually transmitted credit card disclosures are a third.

PHAWKER: www.phawker.com

Q&A: With Online Privacy Expert Lori Andrews

Interview Date: January 12, 2013

Available at: http://www.phawker.com/2012/01/12/qa-with-online-privacy-expert-lori-andrews/

Andrews is a law professor whose work assesses the social impact of emerging technologies. She directs the Institute for Science, Law and Technology at Illinois Institute of Technology, where she teaches a class on the Law of Social Networks. She is the author of 14 books. Her groundbreaking pro bono litigation caused the National Law Journal to list her as one of the 100 Most Influential Lawyers in America.
…

PHAWKER: Getting back to Facebook changing the rules all the time with very little notice—why is that? Why do they constantly make people feel like they are unwillingly in a game of three card monty with their private information?

LORI ANDREWS: I think the users of Facebook think they are the consumers, when they're actually the product. Facebook makes $1.86 billion a year through taking people's private information and making it available, and using it to target ads. So if I email a friend that I'm going to go on vaction in Florida, do a Google search about it, or post something about it on my Facebook page, that becomes information about me that can be marketed to, say, travel agencies, or local attractions in Florida. And so, less privacy is always better for Facebook, because it gives them more information to sell. The more you say, the more they can track you through your friends, and the more, the better.

PHAWKER: We hear a lot about this data mining that you're talking about, that every consumer choice is being recorded somewhere. Does everybody in this country have a vast file being kept on them somewhere?

LORI ANDREWS: Well, there's one company that's called Axciom that has 1500 pieces of information on 96% of Americans. Their former CEO has called it "the biggest company you never heard of." They have everything from your political party, to whether you've ever taken drugs for incontinence. And some of the ways in which data aggregators get this information is by putting cookies, or web beacons, or flash cookies on your computer. And, amazingly, when consumers have gone to court and said "that marketing group should not be collecting information about me without my consent," courts have said it doesn't violate wire tap laws, or the Computer Fraud and Abuse Act, or any of these federal laws because the courts have said one party's consent is enough. And so if Facebook, or Amazon, or Dictionary.com says it's OK for a third party company to collect information about you—that's fine. The company doesn't have to ask you for your personal consent. And I think that's wrong—it's your information, they should have to ask you about collecting it.

And the most troubling thing that in California now, an ad company called NebuAd has made deals with Internet service providers to put hardware on the ISP's network to collect every transmission that every Internet user on that ISP makes. Every email, every Skype call, every search on the web. And what NebuAd said when they were sued for various privacy invasions, was that if we can't be liable under these federal laws because we have the ISP's consent, and therefore don't need the consumer's consent, how can we be liable under the state laws in California, which actually has a Constitutional privacy provision. Now that case will likely settle, and we won't have any precedent. But to me, that is amazing! When I go to make a purchase, when I put my social security number in to get a fishing license, or use my credit card to order a flight on Southwest Airlines, or email my doctor about a prescription change, I don't think that the company is going to pick that up, and use it to market things.

PHAWKER: Hasn't the groundwork for that already been laid, with the way the NSA currently hoovers up all web traffic and keeps it in massive databases? If they want they could look at every e-mail you ever sent, every web search…

LORI ANDREWS: I do, in my book, talk about the 350 search terms that Homeland Security looks for in your e-mails — but that's different, in that they don't make it available to potential employers. They're not commercializing my data, which I find really problematic.

PHAWKER: Aren't we already pretty far down the slippery slope? Five years ago when all this was made public information, that the federal government had made arrangements with every major carrier (AT&T, Verizon, etc.) to put taps on everything, and the American public just kind of shrugged.

LORI ANDREWS: I think we should totally fight for those rights in both areas, vis-à-vis government, and the commercial sector. For example, I do not think the cops should be able to get information from social networks without a warrant. That's another area where I think the rules should apply as they apply offline. It's the 225th anniversary of the U.S. Constitution, which is why I'm excited about launching the book in Philadelphia where the Constitution was drafted. I'm advocating a Constitution for social networks that is very much about applying those Constitutional rights we already have to a new setting.
…

PHAWKER: Why are none of these things we are talking about being addressed by Congress? I'm asking this question rhetorically because I already know the answer: Because Facebook and other big data companies give massive amounts of money to congressional candidates and hire lobbyists to strong arm any that that can't buy. If campaigns were publicly financed, and corporate special interests couldn't give politicians any money, do you think a lot of these things you're talking about would actually have been addressed a while ago?

LORI ANDREWS: I think certainly it would make a difference to have publicly funded campaigns. I think also many people don't know this is going on. Until I started this book, I didn't know about data aggregators. I didn't know about sites like Spokeo.com,, where you enter a person's name, and it'll tell you their estimated worth for a free subscription, and then for more money, they say they can give you any photos that are published on the web. So part of it is that

we don't even realize that this is happening to us, and there are a couple people in Congress—Al Franken, Patrick Leahy—who are trying to do something, but often what they're trying to do is very narrow, like limiting law enforcement use. So we really need someone to come up with a more comprehensive approach to what's going on, and ways to handle it. That's why I thought "the Constitution," which people are really aware of. They know about the Miranda rights, and so forth, and I think we should have a similar kind of warning system, that says, "you have the right to remain silent."

PHAWKER: Dictionary.com is one of the most aggressive, in terms of putting cookies on you, is that correct?

LORI ANDREWS: They put 233 cookies on your computer when you use their web site, according to The Wall Street Journal.

PHAWKER: Jesus! Is there a "silver bullet" solution to all this, or is it going to be incremental—one thing at a time?

LORI ANDREWS: I think we should change the default position—no data collection, unless we opt in—that would take care of a lot of this. And then maybe some laws about third parties, for example, employers can't Google an applicant, and then not hire them based on what they find there.

Payless ShoeSource: www.payless.com/store/

Payless ShoeSource Privacy Policy

Available at: http://www.payless.com/store/home/privacy.jsp

We value our customers and respect their privacy. We seek to provide products, services, and valuable offers to you and your family. We collect information from our interactions with you, other customers and other parties to help us achieve that goal. Your privacy is important to us. As described in this Privacy Policy, we do, however, share your personal information with our affiliates and certain third parties who provide services on our behalf.

In this policy we use 'we' to mean Payless ShoeSource, Inc. We are part of the Collective Brands family of companies and there are details of the other members of the group here http://www.collectivebrands.com/business-units/

We have made this Privacy Policy available to you to let you know what kind of personal information we collect, how it is handled, with whom it may be shared, and how you may access the data you provide to us. This policy governs how we collect, use and disseminate the personal information we collect from and about you. Our policy also describes the choices you can make about the way your personal information is collected and used. By visiting any part of our web site (the "Website"), you consent to the policies and practices described in this Privacy Policy and the Terms of Use of our Websites, which are incorporated herein by reference.
…
Types of Information We Collect and How We Collect It

We collect information such as your name, email, postal address, phone number, and billing and credit card information when you register this information with our Website; make an in-store purchase or provide this information in a store; place an order on-line; save your information with us online; use a mobile application; or participate in sweepstakes, contests, promotions or surveys. We may combine information about you that we have with information we obtain from business partners or other companies. You may choose not to provide certain information, but choosing to do so may prevent you from being able to take advantage of many of our Website's features or from conducting transactions.

When you submit a question to customer service, we may need your email address to respond, and you may also provide us with additional information to help us answer your question.

We maintain a record of your product interests and the purchases you make in our stores or on-line, and may secure information about you from our joint marketing partners or from unrelated third parties. We may also collect demographic information, and we may use mailing lists from third parties. Whenever you browse our site, we automatically receive and record information, such as your IP address, browser type, domain name and specific web pages through which you click.

We use computer "cookies" (small files placed on your hard drive) to make your shopping experience more efficient, convenient and personalized. Cookies are alphanumeric identifiers that enable our systems to recognize your browser and share information with your computer. Through the use of these cookies, we may automatically collect information and data, such as your IP address, browser type, domain name and specific web pages through which you click. Cookies are not required for you to browse our site, but they are required to add items to your shopping cart and for you to place an order. Cookies should not contain personal data other than your IP address. The Help portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. However, cookies allow you to take full advantage of some of our Website's features, and we recommend that you leave them turned on. By using the site you consent to our use of cookies. To learn more about cookies and how to use them visit the Help portion of your internet browser.

We may also use third party companies to place advertising at other sites across the Internet. These advertising companies collect information about your visits to our Website or interaction with our email through the use of "web beacons". This technology allows them to use information about your visits to this and other web sites to help us serve you better. We also use web beacons to review how visitors navigate the Website or interact with our email advertising. If you would like more information about this practice, and your choices and they relate to this practice, please contact us. To provide location-based services on our Website and through any mobile applications we use we may need to capture and record location data regarding your use of the Website or mobile applications and your travels to provide location-related functionality ("Location-Data"). We may link that Location-Data to other information that you provide to us or that may be accessed in connection with your use of the Website or the mobile applications. Your use of, and our ability to offer functionality through, the Website or mobile applications is then enabled through our use and disclosure to third parties of Location-Data and associated information. How We Use Your Information.

Our primary purpose for collecting personal information is for us to provide you with a safe, efficient and beneficial experience. We may use your personal information for the purpose of improving our services and our Website's contents or mobile application layout and functionality; to inform you about future marketing, service updates and promotional offers; to communicate preferences which you have indicated; to customize the advertising and content you see and improve future shopping for you; to determine whether you are eligible for an offer; to verify information; to improve our services, or for any other purpose disclosed at the point of collection. We may also use your information to provide services and customer support that you may request, as well as to correct problems, resolve disputes and collect fees.

When you browse our Website or make a purchase online, the information recorded and collected automatically, such as your IP address, browser type, domain name and specific web pages through which you click, is used in aggregate to help us look for trends so that we can improve our Website and your browsing experience. These statistics may also be used in communications, such as our annual report, but we do not identify individuals in these communications.

When you purchase items from us, we use your personal information to process and fulfill your order, send you emails to notify you of order status, or to contact you by phone, postal mail or email if we have questions regarding your order or purchase.

When you register with us or when you make a purchase at a store or one of our Websites, we may use your personal information to send you information and updates about new products, special sales and promotions related to your purchase, and to help us learn more about your shopping preferences. These communications may be sent via email, postal mail, telephone text message, or through a mobile application. You always have the choice to opt-out of receiving these marketing communications.

If you participate in a sweepstakes, contest or promotion, on-line, over the phone, through a mobile application or at one of our stores, we may use your personal information to contact you via email, postal mail, telephone, text message, or through a mobile application regarding our products, services, contests and promotions. You may choose at any time not to receive these marketing communications. We may still need to contact you on a limited basis, however - for example, to notify winners and to fulfill promotional obligations.

We may also use the information we collect on our Website as necessary to comply with legal requirements, to enforce the Website terms of use, to prevent fraud, to co-operate with law enforcement and regulatory authorities and to stop other prohibited, illegal or harmful activities. We share information across the Collective Brands family and we may use servers and resources of other members of the group to process your data. Our main servers are in Topeka, Kansas, USA and it is likely that your data will be held on servers there and at other Collective Brands locations around the world. When you provide us with your personal data, you acknowledge that this information may be stored and processed on servers located outside the European Economic Area ('EEA') and you consent to your personal data being exported outside the EEA and being stored and processed at our discretion on any of Collective Brands' servers wherever located.

Our Disclosure of Your Information

We may combine your information with information we collect from other companies (such as demographic data) to improve and personalize our services. We may also use third-party companies to assist in collection and analysis of data collected through the use of web beacons. We may share your personal information with affiliated companies that are subject to privacy policies consistent with this policy.

We may also share your personal information with outside companies that perform services specifically for Collective Brands group. We may employ independent contractors, vendors and suppliers to provide specific services and products. For example, we may retain an outside company to create and distribute a direct mail or email offering. Other examples include fulfilling orders, delivering packages, sending postal mail, email, or text messages, communicating with our customers, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, fraud screening, translation services and providing customer service. They may sometimes have access to information collected by

us, including your personal data, in the course of providing products or services to us. In those situations, the outside company is performing work for us, and we take appropriate steps designed to ensure that your personal information is used only to provide the services requested by us.

We may also disclose that personal information to third-parties to whom you explicitly ask us to send your information.

If we sell or buy any business or assets (in whole or in part), we may disclose your personal data to the prospective sellers or buyers of the business or assets and their advisors. If Collective Brands or some of its assets are acquired by a third party, the data held will be one of the transferred assets. Similarly, your personal information may be passed on to a successor in interest in the event of a reorganization, reconstruction, liquidation, bankruptcy or administration. It may be that any buyer or successor buys all or only part of our business. It may also be the case that they are not in the same line of business as us. If this is the case we will expect them to observe the terms of this privacy policy.

We reserve the right to release account and other personal information about you when we believe release is appropriate to comply with the law, in response to legal process and law enforcement requests, to enforce or apply our Terms of Use and other agreements, or to protect our rights, property, safety or other interests those of our parent company, affiliates and shareholders, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction.

Any personal information shared via any mobile application or on another website (such as Facebook, YouTube, Google+ or Twitter) may become public information. We cannot control the use of information disclosed in public forums, such as forums, bulletin boards, blogs, chat rooms, and networking functions of mobile applications. You should exercise caution when disclosing information in these public areas, especially your Location-Data, and be careful how you disclose your Personal Information. Content posted in public areas of our mobile applications, including advice and opinions, represents the views and is the responsibility of those who post the content. We do not necessarily endorse, support, verify, or agree with the content posted. If you have any questions or comments about any content on our mobile applications please contact our Customer Service Center.

…

Amendments to Our Privacy Policy

We reserve the right to change our Privacy Policy as our business changes. If our policy changes in the future, we will post an updated privacy policy on our Website. You can tell if this policy has changed by checking the revision date that appears at the end of this policy. If you would like a permanent record of this privacy policy please print a copy.

Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS

FTC REPORT
MARCH 2012

CONTENTS

EXECUTIVE SUMMARY

In today's world of smart phones, smart grids, and smart cars, companies are collecting, storing, and sharing more information about consumers than ever before. Although companies use this information to innovate and deliver better products and services to consumers, they should not do so at the expense of consumer privacy.

With this Report, the Commission calls on companies to act now to implement best practices to protect consumers' private information. These best practices include making privacy the "default setting" for commercial data practices and giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency. Implementing these best practices will enhance trust and stimulate commerce.

This Report follows a preliminary staff report that the Federal Trade Commission ("FTC" or "Commission") issued in December 2010. The preliminary report proposed a framework for protecting consumer privacy in the 21st Century. Like this Report, the framework urged companies to adopt the following practices, consistent with the Fair Information Practice Principles first articulated almost 40 years ago:

- **Privacy by Design:** Build in privacy at every stage of product development;
- **Simplified Choice for Businesses and Consumers:** Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism, while reducing the burden on businesses of providing unnecessary choices; and
- **Greater Transparency:** Make information collection and use practices transparent.

The Commission received more than 450 public comments in response to the preliminary report from various stakeholders, including businesses, privacy advocates, technologists and individual consumers. A wide range of stakeholders, including industry, supported the principles underlying the framework, and many companies said they were already following them. At the same time, many commenters criticized the slow pace of self-regulation, and argued that it is time for Congress to enact baseline privacy legislation. In this Report, the Commission addresses the comments and sets forth a revised, final privacy framework that adheres to, but also clarifies and fine-tunes, the basic principles laid out in the preliminary report.

Since the Commission issued the preliminary staff report, Congress has introduced both general privacy bills and more focused bills, including ones addressing Do Not Track and the privacy of teens. Industry has made some progress in certain areas, most notably, in responding to the preliminary report's call for Do Not Track. In other areas, however, industry progress has been far slower. Thus, overall, consumers do not yet enjoy the privacy protections proposed in the preliminary staff report.

The Administration and certain Members of Congress have called for enactment of baseline privacy legislation. The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

The remainder of this Executive Summary describes key developments since the issuance of the preliminary report, discusses the most significant revisions to the proposed framework, and lays out several next steps.

DEVELOPMENTS SINCE ISSUANCE OF THE PRELIMINARY REPORT

In the last 40 years, the Commission has taken numerous actions to shape the consumer privacy landscape. For example, the Commission has sued dozens of companies that broke their privacy and security promises, scores of telemarketers that called consumers on the Do Not Call registry, and more than a hundred scammers peddling unwanted spam and spyware. Since it issued the initial staff report, the Commission has redoubled its efforts to protect consumer privacy, including through law enforcement, policy advocacy, and consumer and business education. It has also vigorously promoted self-regulatory efforts.

On the law enforcement front, since December 2010, the Commission:

- Brought enforcement actions against Google and Facebook. The orders obtained in these cases require the companies to obtain consumers' affirmative express consent before materially changing certain of their data practices and to adopt strong, company-wide privacy programs that outside auditors will assess for 20 years. These orders will protect the more than one billion Google and Facebook users worldwide.
- Brought enforcement actions against online advertising networks that failed to honor opt outs. The orders in these cases are designed to ensure that when consumers choose to opt out of tracking by advertisers, their choice is effective.
- Brought enforcement actions against mobile applications that violated the Children's Online Privacy Protection Act as well as applications that set default privacy settings in a way that caused consumers to unwittingly share their personal data.
- Brought enforcement actions against entities that sold consumer lists to marketers in violation of the Fair Credit Reporting Act.
- Brought actions against companies for failure to maintain reasonable data security.

On the policy front, since December 2010, the FTC and staff:

- Hosted two privacy-related workshops, one on child identity theft and one on the privacy implications of facial recognition technology.
- Testified before Congress ten times on privacy and data security issues.
- Consulted with other federal agencies, including the Federal Communications Commission, the Department of Health and Human Services, and the Department of Commerce, on their privacy initiatives. The Commission has supported the Department of Commerce's initiative to convene stakeholders to develop privacy-related codes of conduct for different industry sectors.
- Released a survey of data collection disclosures by mobile applications directed to children.
- Proposed amendments to the Children's Online Privacy Protection Act Rule.

On the education front, since December 2010, the Commission:

- Continued outreach efforts through the FTC's consumer online safety portal, OnGuardOnline.gov, which provides information in a variety of formats – articles, games, quizzes, and videos – to help consumers secure their computers and protect their personal information. It attracts approximately 100,000 unique visitors per month.
- Published new consumer education materials on identity theft, Wi-Fi hot spots, cookies, and mobile devices.
- Sent warning letters to marketers of mobile apps that do background checks on individuals, educating them about the requirements of the Fair Credit Reporting Act.

To promote self-regulation, since December 2010, the Commission:

- Continued its call for improved privacy disclosures and choices, particularly in the area of online behavioral tracking. In response to this call, as well as to Congressional interest:
  - A number of Internet browser vendors developed browser-based tools for consumers to request that websites not track their online activities.
  - The World Wide Web Consortium, an Internet standard setting organization, is developing a universal web protocol for Do Not Track.
  - The Digital Advertising Alliance ("DAA"), a coalition of media and marketing organizations, has developed a mechanism, accessed through an icon that consumers can click, to obtain information about and opt out of online behavioral advertising. Additionally, the DAA has committed to preventing the use of consumers' data for secondary purposes like credit and employment and honoring the choices about tracking that consumers make through the settings on their browsers.
- Participated in the development of enforceable cross-border privacy rules for businesses to harmonize and enhance privacy protection of consumer data that moves between member countries of the forum on Asia Pacific Economic Cooperation.

THE FINAL REPORT

Based upon its analysis of the comments filed on the proposed privacy framework, as well as commercial and technological developments, the Commission is issuing this final Report. The final framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC. While retaining the proposed framework's fundamental best practices of privacy by design, simplified choice, and greater transparency, the Commission makes revised recommendations in three key areas in response to the comments.

First, the Commission makes changes to the framework's scope. The preliminary report proposed that the privacy framework apply to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. To address concerns about undue burdens on small businesses, the final framework does not apply to companies that collect only non-sensitive data from fewer than 5,000 consumers a year, provided they do not share the data with third parties. Commenters also expressed concern that, with improvements in technology and the ubiquity of public information, more and more data could be "reasonably linked" to a consumer, computer or device, and that the proposed framework provided less incentive for a business to try to de-identify the data it maintains. To address this issue, the Report clarifies that data is not "reasonably linkable" to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.

Second, the Commission revises its approach to how companies should provide consumers with privacy choices. To simplify choice for both consumers and businesses, the proposed framework set forth a list of five categories of "commonly accepted" information collection and use practices for which companies need not provide consumers with choice (product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing). Several business commenters expressed concern that setting these "commonly accepted practices" in stone would stifle innovation. Other commenters expressed the concern that the "commonly accepted practices" delineated in the proposed framework were too broad and would allow a variety of practices to take place without consumer consent.

In response to these concerns, the Commission sets forth a modified approach that focuses on the context of the consumer's interaction with the business. Under this approach, companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law. Although many of the five "commonly accepted practices" identified in the preliminary report would generally meet this standard, there may be exceptions. The Report provides examples of how this new "context of the interaction" standard would apply in various circumstances.

Third, the Commission recommends that Congress consider enacting targeted legislation to provide greater transparency for, and control over, the practices of information brokers. The proposed framework recommended that companies provide consumers with reasonable access to the data the companies maintain about them, proportionate to the sensitivity of the data and the nature of its use. Several commenters discussed in particular the importance of consumers' ability to access information that information brokers have about them. These commenters noted the lack of transparency about the practices of information brokers, who often buy, compile, and sell a wealth of highly personal information about consumers but never interact directly with them. Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.

The Commission agrees that consumers should have more control over the practices of information brokers and believes that appropriate legislation could help address this goal. Any such legislation could be

modeled on a bill that the House passed on a bipartisan basis during the 111th Congress, which included a procedure for consumers to access and dispute personal data held by information brokers.

IMPLEMENTATION OF THE PRIVACY FRAMEWORK

While Congress considers privacy legislation, the Commission urges industry to accelerate the pace of its self-regulatory measures to implement the Commission's final privacy framework. Although some companies have excellent privacy and data security practices, industry as a whole must do better. Over the course of the next year, Commission staff will promote the framework's implementation by focusing its policymaking efforts on five main action items, which are highlighted here and discussed further throughout the report.

- **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the Digital Advertising Alliance ("DAA") has developed its own icon-based tool and has committed to honor the browser tools; and the World Wide Web Consortium ("W3C") has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.
- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.
- **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media seek, to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

- **Promoting Enforceable Self-Regulatory Codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

FINAL FTC PRIVACY FRAMEWORK AND IMPLEMENTATION RECOMMENDATIONS

The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

SCOPE

Final Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.

PRIVACY BY DESIGN

Baseline Principle: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

A. The Substantive Principles

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

B. Procedural Protections to Implement the Substantive Principles

Final Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

SIMPLIFIED CONSUMER CHOICE

Baseline Principle: Companies should simplify consumer choice.

A. Practices That Do Not Require Choice

Final Principle: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law.

To balance the desire for flexibility with the need to limit the types of practices for which choice is not required, the Commission has refined the final framework so that companies engaged in practices consistent with the context of their interaction with consumers need not provide choices for those practices.

B. Companies Should Provide Consumer Choice for Other Practices

Final Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.

The Commission commends industry's efforts to improve consumer control over online behavioral tracking by developing a Do Not Track mechanism, and encourages continued improvements and full implementation of those mechanisms.

TRANSPARENCY

Baseline Principle: Companies should increase the transparency of their data practices.

A. Privacy notices

Final Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

B. Access

Final Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

The Commission has amplified its support for this principle by including specific recommendations governing the practices of information brokers.

C. Consumer Education

Final Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

LEGISLATIVE RECOMMENDATIONS

The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security and data broker legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

FTC WILL ASSIST WITH IMPLEMENTATION IN FIVE KEY AREAS

As discussed throughout the Commission's final Report, there are a number of specific areas where policy makers have a role in assisting with the implementation of the self-regulatory principles that make up the final privacy framework. Areas where the FTC will be active over the course of the next year include the following:

1. Do Not Track

Industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.

2. Mobile

The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

3. Data Brokers

To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.

4. Large Platform Providers

To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

5. Promoting Enforceable Self-Regulatory Codes

The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

In all other areas, the Commission calls on individual companies, trade associations, and self-regulatory bodies to adopt the principles contained in the final privacy framework, to the extent they have not already done so. For its part, the FTC will focus its policy efforts on the five areas identified above, vigorously enforce existing laws, work with industry on self-regulation, and continue to target its education efforts on building awareness of existing data collection and use practices and the tools to control them.

I. INTRODUCTION

In December 2010, the Federal Trade Commission ("FTC" or "Commission") issued a preliminary staff report to address the privacy issues associated with new technologies and business models.[1] The report outlined the FTC's 40-year history of promoting consumer privacy through policy and enforcement work, discussed the themes and areas of consensus that emerged from the Commission's "Exploring Privacy" roundtables, and set forth a proposed framework to guide policymakers and other stakeholders regarding best practices for consumer privacy. The proposed framework called on companies to build privacy protections into their business operations (*i.e.*, adopt "privacy by design"[2]), offer simplified choice mechanisms that give consumers more meaningful control, and increase the transparency of their data practices.

The preliminary report included a number of questions for public comment to assist and guide the Commission in developing a final privacy framework. The Commission received more than 450 comments from a wide variety of interested parties, including consumer and privacy advocates, individual companies and trade associations, academics, technologists, and domestic and foreign government agencies. Significantly, more than half of the comments came from individual consumers. The comments have helped the Commission refine the framework to better protect consumer privacy in today's dynamic and rapidly changing marketplace.

In this Final Report, the Commission adopts staff's preliminary framework with certain clarifications and revisions. The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

The Report highlights the developments since the FTC issued staff's preliminary report, including the Department of Commerce's parallel privacy initiative, proposed legislation, and actions by industry and other stakeholders. Next, it analyzes and responds to the main issues raised by the public comments. Based on those comments, as well as marketplace developments, the Report sets forth a revised privacy framework and legislative recommendations. Finally, the Report outlines a series of policy initiatives that FTC staff will undertake in the next year to assist industry with implementing the final framework as best practices.

1 FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report* (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

2 Privacy by Design is an approach that Ann Cavoukian, Ph.D., Information and Privacy Commissioner, Ontario, Canada, has advocated. *See* Information and Privacy Commissioner, Ontario, Canada, Privacy by Design, http://privacybydesign.ca/.

II. BACKGROUND

A. FTC ROUNDTABLES AND PRELIMINARY STAFF REPORT

Between December 2009 and March 2010, the FTC convened its "Exploring Privacy" roundtables.[3] The roundtables brought together stakeholders representing diverse interests to evaluate whether the FTC's existing approach to protecting consumer privacy was adequate in light of 21st Century technologies and business models. From these discussions, as well as submitted materials, a number of themes emerged. First, the collection and commercial use of consumer data in today's society is ubiquitous and often invisible to consumers. Second, consumers generally lack full understanding of the nature and extent of this data collection and use and, therefore, are unable to make informed choices about it. Third, despite this lack of understanding, many consumers are concerned about the privacy of their personal information. Fourth, the collection and use of consumer data has led to significant benefits in the form of new products and services. Finally, the traditional distinction between personally identifiable information and "anonymous" data has blurred.

Participants also pointed to shortcomings in existing frameworks that have attempted to address privacy concerns. The "notice-and-choice model," which encouraged companies to develop privacy policies describing their information collection and use practices, led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand.[4] The "harm-based model," which focused on protecting consumers from specific harms – physical security, economic injury, and unwarranted intrusions into their daily lives – had been criticized for failing to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored.[5] Participants noted that both of these privacy frameworks have struggled to keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers' information in ways that often are invisible to consumers.[6]

Building on the record developed at the roundtables and on its own enforcement and policymaking expertise, FTC staff proposed for public comment a framework for approaching privacy. The proposed framework included three major components. It called on companies to treat privacy as their "default setting" by implementing "privacy by design" throughout their regular business operations. The concept of privacy by design includes limitations on data collection and retention, as well as reasonable security and data accuracy. By considering and addressing privacy at every stage of product and service development,

3 The first roundtable took place on December 7, 2009, the second roundtable on January 28, 2010, and the third roundtable on March 17, 2010. *See* FTC, *Exploring Privacy – A Roundtable Series*, http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

4 *See, e.g., 1st Roundtable, Remarks of Fred Cate, Indiana University Maurer School of Law*, at 280-81; *1st Roundtable, Remarks of Lorrie Cranor, Carnegie Mellon University*, at 129; *see also Written Comment of Fred Cate*, *2nd Roundtable, Consumer Protection in the Age of the 'Information Economy,'* cmt. #544506-00057, at 343-79.

5 *See, e.g., 1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center*, at 301; *1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 36-38; *1st Roundtable, Remarks of Susan Grant, Consumer Federation of America*, at 38-39.

6 *See, e.g., 3rd Roundtable, Remarks of Kathryn Montgomery, American University School of Communication*, at 200-01; *2nd Roundtable, Remarks of Kevin Bankston, Electronic Frontier Foundation*, at 277.

companies can shift the burden away from consumers who would otherwise have to seek out privacy-protective practices and technologies. The proposed framework also called on companies to simplify consumer choice by presenting important choices – in a streamlined way – to consumers at the time they are making decisions about their data. As part of the call for simplified choice, staff asked industry to develop a mechanism that would allow consumers to more easily control the tracking of their online activities, often referred to as "Do Not Track." Finally, the framework focused on improving consumer understanding of commercial data practices ("transparency") and called on companies – both those that interact directly with consumers and those that lack a consumer interface – to improve the transparency of their practices. As discussed below, the Commission received a large number of thoughtful and informative comments regarding each of the framework's elements. These comments have allowed the Commission to refine the framework and to provide further guidance regarding its implementation.

B. DEPARTMENT OF COMMERCE PRIVACY INITIATIVES

In a related effort to examine privacy, in May 2010, the Department of Commerce ("DOC" or "Commerce") convened a public workshop to discuss how to balance innovation, commerce, and consumer privacy in the online context.[7] Based on the input received from the workshop, as well as related research, on December 16, 2010, the DOC published for comment a strategy paper outlining privacy recommendations and proposed initiatives.[8] Following the public comment period, on February 23, 2012, the Administration issued its final "White Paper" on consumer privacy. The White Paper recommends that Congress enact legislation to implement a Consumer Privacy Bill of Rights based on the Fair Information Practice Principles ("FIPPs").[9] In addition, the White Paper calls for a multistakeholder process to determine how to apply the Consumer Privacy Bill of Rights in different business contexts. Commerce issued a Notice of Inquiry on March 5, 2012, asking for public input on both the process for convening stakeholders on this project, as well as the proposed subject areas to be discussed.[10]

Staff from the FTC and Commerce worked closely to ensure that the agencies' privacy initiatives are complementary. Personnel from each agency actively participated in both the DOC and FTC initiatives, and have also communicated regularly on how best to develop a meaningful, effective, and consistent approach to privacy protection. Going forward, the agencies will continue to work collaboratively to guide implementation of these complementary privacy initiatives.

7 *See* Press Release, Department of Commerce, Commerce Secretary Gary Locke Discusses Privacy and Innovation with Leading Internet Stakeholders (May 7, 2010), *available at* http://www.commerce.gov/news/press-releases/2010/05/07/commerce-secretary-gary-locke-discusses-privacy-and-innovation-leadin.

8 *See* Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010), *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

9 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The FIPPs as articulated in the Administration paper are: Transparency, Individual Control, Respect for Context, Security, Access, Accuracy, Focused Collection, and Accountability.

10 *See* National Telecommunications and Information Administration, Request for Public Comment, Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 13098 (Mar. 5, 2012).

C. LEGISLATIVE PROPOSALS AND EFFORTS BY STAKEHOLDERS

Since Commission staff released its preliminary report in December 2010, there have been a number of significant legislative proposals, as well as steps by industry and other stakeholders, to promote consumer privacy.

1. DO NOT TRACK

The preliminary staff report called on industry to create and implement a mechanism to allow consumers to control the collection and use of their online browsing data, often referred to as "Do Not Track." Bills introduced in the House and the Senate specifically address the creation of Do Not Track mechanisms, and, if enacted, would mandate that the Commission promulgate regulations to establish standards for a Do Not Track regime.[11]

In addition to the legislative proposals calling for the creation of Do Not Track, staff's preliminary report recommendation triggered significant progress by various industry sectors to develop tools to allow consumers to control online tracking. A number of browser vendors – including Mozilla, Microsoft, and Apple – announced that the latest versions of their browsers permit consumers to instruct websites not to track their activities across websites.[12] Mozilla has also introduced a mobile browser for Android devices that enables Do Not Track.[13] The online advertising industry has also established an important program. The Digital Advertising Alliance ("DAA"), an industry coalition of media and marketing associations, has developed an initiative that includes an icon embedded in behaviorally targeted online ads.[14] When consumers click on the icon, they can see information about how the ad was targeted and delivered to them and they are given the opportunity to opt out of such targeted advertising. The program's recent growth and implementation has been significant. In addition, the DAA has committed to preventing the use of consumers' data for secondary purposes like credit and employment decisions. The DAA has also agreed to honor the choices about tracking that consumers make through settings on their web browsers. This will provide consumers two ways to opt out: through the DAA's icon in advertisements or through their browser settings. These steps demonstrate the online advertising industry's support for privacy and consumer choice.

---

11 *See* Do-Not-Track Online Act of 2011, S. 913, 112th Congress (2011); Do Not Track Me Online Act, H.R. 654, 112th Congress (2011).

12 *See* Press Release, Microsoft, Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9 (Dec. 7, 2010), *available at* http://www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.mspx; *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities*, Mozilla Blog (Feb. 8, 2011), http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/; Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, Wall St. J., Apr. 13, 2011, *available at* http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html. Google recently announced that it will also offer this capability in the next version of its browser. Gregg Kaizer, *FAQ: What Google's Do Not Track Move Means*, Computerworld (Feb. 24, 2012), *available at* http://www.computerworld.com/s/article/9224583/FAQ_What_Google_s_Do_Not_Track_move_means.

13 *See* Mozilla, Do Not Track FAQs, http://dnt.mozilla.org.

14 *See* Press Release, Interactive Advertising Bureau, Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control Over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410.

Finally, the World Wide Web Consortium ("W3C")[15] convened a working group to create a universal standard for Do Not Track. The working group includes DAA member companies, other U.S. and international companies, industry groups, and consumer groups. The W3C group has made substantial progress toward a standard that is workable in the desktop and mobile settings, and has published two working drafts of its standard documents. The group's goal is to complete a consensus standard in the coming months.

2. OTHER PRIVACY INITIATIVES

Beyond the Do Not Track developments, broader initiatives to improve consumer privacy are underway in Congress, Federal agencies, and the private sector. For example, Congress is considering several general privacy bills that would establish a regulatory framework for protecting consumer privacy by improving transparency about the commercial uses of personal information and providing consumers with choice about such use.[16] The bills would also provide the Commission rulemaking authority concerning, among other things, notice, consent, and the transfer of information to third parties.

In the House of Representatives, Members have introduced bipartisan legislation to amend the Children's Online Privacy Protection Act[17] ("COPPA") and establish other protections for children and teens.[18] The bill would prohibit the collection and use of minors' information for targeted marketing and would require websites to permit the deletion of publicly available information of minors. Members of Congress also introduced a number of other bills addressing data security and data breach notification in 2011.[19]

15 The W3C is an international standard-setting body that works "to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web." *See* W3C Mission, http://www.w3.org/Consortium/mission.html.

16 *See* Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Congress (2011); Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 611, 112th Congress (2011); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Congress (2011).

17 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506.

18 *See* Do Not Track Kids Act of 2011, H.R. 1895, 112th Congress (2011). In September 2011, the Commission issued a Notice of Proposed Rulemaking, proposing changes to the COPPA Rule to address changes in technology. *See FTC Children's Online Privacy Protection Rule*, 76 Fed. Reg. 59804 (proposed Sep. 27, 2011), *available at* http://www.ftc.gov/os/2011/09/110915coppa.pdf.

19 *See* Personal Data Privacy and Security Act of 2011, S. 1151, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011); Data Breach Notification Act of 2011, S.1408, 112th Congress (2011); Data Security Act of 2011, S.1434, 112th Congress (2011); Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Congress (2011); Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Secure and Fortify Electronic Data Act, H.R. 2577, 112th Congress (2011).

Federal agencies have taken significant steps to improve consumer privacy as well. For its part, since issuing the preliminary staff report, the FTC has resolved seven data security cases,[20] obtained orders against Google, Facebook, and online ad networks,[21] and challenged practices that violate sector-specific privacy laws like the Fair Credit Reporting Act ("FCRA") and COPPA.[22] The Commission has also proposed amendments to the COPPA Rule to address changes in technology. The comment period on the Proposed Rulemaking ran through December 23, 2011, and the Commission is currently reviewing the comments received.[23] Additionally, the Commission has hosted public workshops on discrete privacy issues such as child identity theft and the use of facial recognition technology.

Other federal agencies have also begun examining privacy issues. In 2011, the Federal Communications Commission ("FCC") hosted a public forum to address privacy concerns associated with location-based services.[24] The Department of Health and Human Services ("HHS") hosted a forum on medical identity theft, developed a model privacy notice for personal health records,[25] and is developing legislative recommendations on privacy and security for such personal health records. In addition, HHS recently launched an initiative to identify privacy and security best practices for using mobile devices in health care settings.[26]

---

20 *See In the Matter of Upromise, Inc.,* FTC File No. 102 3116 (Jan. 18, 2012) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/1023116/index.shtm; *In the Matter of ACRAnet, Inc.*, FTC Docket No. C-4331 (Aug. 17, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923088/index.shtm; *In the Matter of SettlementOne Credit Corp.*, FTC Docket No. C-4330 (Aug. 17, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0823208/index.shtm; *In the Matter of Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023160/index.shtm; *In the Matter of Lookout Servs., Inc.,* FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023076/index.shtm; *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923093/index.shtm; *In the Matter of Fajilan & Assocs., Inc.,* FTC Docket No. C-4332 (Aug. 17, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923089/index.shtm.

21 *See In the Matter of Google, Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023136/index.shtm (requiring company to implement privacy program subject to independent third-party audit); *In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/index.shtm (requiring company to implement privacy program subject to independent third-party audit); *In the Matter of Chitika, Inc.*, FTC Docket No. C-4324 (June 7, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023087/index.shtm (requiring company's behavioral advertising opt out to last for five years); *In the Matter of ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 14, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023185/index.shtm (requiring company to improve disclosure of its data collection practices and offer consumers a user-friendly opt out mechanism).

22 Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*; COPPA Rule, 16 C.F.R. Part 312; *see also, e.g.*, *United States v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Cal. Sept. 8, 2011) (COPPA consent decree); *United States v. Teletrack, Inc.*, No. 1 11-CV-2060 (N.D. Ga. filed June 24, 2011) (FCRA consent decree); *United States v. Playdom, Inc.*, No. SACV-11-00724-AG (ANx) (C.D. Cal. May 24, 2011) (COPPA consent decree).

23 *See* Press Release, FTC Extends Deadline for Comments on Proposed Amendments to the Children's Online Privacy Protection Rule Until December 23 (Nov. 18, 2011), *available at* http://www.ftc.gov/opa/2011/11/coppa.shtm.

24 *See* FCC Workshop, *Helping Consumers Harness the Potential of Location-Based Services* (June 28, 2011), *available at* http://www.fcc.gov/events/location-based-services-forum.

25 *See* The Office of the National Coordinator for Health Information Technology, Personal Health Record (PHR) Model Privacy Notice, http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__draft_phr_model_notice/1176.

26 *See* HHS Workshop, *Mobile Devices Roundtable: Safeguarding Health Information*, *available at* http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__mobile_devices_roundtable/3815.

The private sector has taken steps to enhance user privacy and security as well. For example, Google and Facebook have improved authentication mechanisms to give users stronger protection against compromised passwords.[27] Also, privacy-enhancing technologies such as the HTTPS Everywhere browser add-on have given users additional tools to encrypt their information in transit.[28] On the mobile front, the Mobile Marketing Association released its Mobile Application Privacy Policy.[29] This document provides guidance on privacy principles for application ("app") developers and discusses how to inform consumers about the collection and use of their data. Despite these developments, as explained below, industry still has more work to do to promote consumer privacy.

III. MAIN THEMES FROM COMMENTERS

The more than 450 comments filed in response to the preliminary staff report addressed three overarching issues: how privacy harms should be articulated; the value of global interoperability of different privacy regimes; and the desirability of baseline privacy legislation to augment self-regulatory efforts. Those comments, and the Commission's analysis, are discussed below.

A. ARTICULATION OF PRIVACY HARMS

There was broad consensus among commenters that consumers need basic privacy protections for their personal information. This is true particularly in light of the complexity of the current personal data ecosystem. Some commenters also stated that the Commission should recognize a broader set of privacy harms than those involving physical and economic injury.[30] For example, one commenter cited complaints from consumers who had been surreptitiously tracked and targeted with prescription drug offers and other health-related materials regarding sensitive medical conditions.[31]

At the same time, some commenters questioned whether the costs of broader privacy protections were justified by the anticipated benefits.[32] Relatedly, many commenters raised concerns about how wider privacy protections would affect innovation and the ability to offer consumers beneficial new products and services.[33]

---

27 *See Advanced Sign-In Security For Your Google Account*, Google Official Blog (Feb. 10, 2011, 11:30 AM), http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html#!/2011/02/advanced-sign-in-security-for-your.html; Andrew Song, *Introducing Login Approvals*, Facebook Blog (May 12, 2011, 9:58 AM), http://www.facebook.com/note.php?note_id=10150172618258920.

28 *See HTTPS Everywhere*, Electronic Frontier Foundation, https://www.eff.org/https-everywhere.

29 *See* Press Release, Mobile Marketing Association, Mobile Marketing Association Releases Final Privacy Policy Guidelines for Mobile Apps (Jan. 25, 2012), *available at* http://mmaglobal.com/news/mobile-marketing-association -releases-final-privacy-policy-guidelines-mobile-apps.

30 *See Comment of TRUSTe*, cmt. #00450, at 3; *Comment of Berlin Commissioner for Data Protection & Freedom of Information*, cmt. #00484, at 1.

31 *See Comment of Patient Privacy Rights*, cmt. #00470, at 2.

32 *See Comment of Technology Policy Institute*, cmt. #00301, at 5-8; *Comment of Experian*, cmt. #00398, at 9-11; *Comment of Global Privacy Alliance*, cmt. #00367, at 6-7.

33 *See Comment of Facebook, Inc.,* cmt. #00413, at 1-2, 7-8; *Comment of Google, Inc.*, cmt. #00417, at 4; *Comment of Global Privacy Alliance*, cmt. #00367, at 16.

The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. These harms may include the unexpected revelation of previously private information, including both sensitive information (*e.g.*, health information, precise geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties.[34] As one example, in the Commission's case against Google, the complaint alleged that Google used the information of consumers who signed up for Gmail to populate a new social network, Google Buzz.[35] The creation of that social network in some cases revealed previously private information about Gmail users' most frequent email contacts. Similarly, the Commission's complaint against Facebook alleged that Facebook's sharing of users' personal information beyond their privacy settings was harmful.[36] Like these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions.[37]

In terms of weighing costs and benefits, although it recognizes that imposing new privacy protections will not be costless, the Commission believes doing so not only will help consumers but also will benefit businesses by building consumer trust in the marketplace. Businesses frequently acknowledge the importance of consumer trust to the growth of digital commerce[38] and surveys support this view. For

34 One former FTC Chairman, in analyzing a spyware case, emphasized that consumers should have control over what is on their computers. Chairman Majoras issued the following statement in connection with the Commission's settlement against Sony BMG resolving claims about the company's installation of invasive tracking software: "Consumers' computers belong to them, and companies must adequately disclose unexpected limitations on the customary use of their products so consumers can make informed decisions regarding whether to purchase and install that content." Press Release, FTC, Sony BMG Settles FTC Charges (Jan. 30, 2007), *available at* http://www.ftc.gov/opa/2007/01/sony.shtm; *see also* Walt Mossberg, *Despite Others' Claims, Tracking Cookies Fit My Spyware Definition*, AllThingsD (July 14, 2005, 12:01 AM), http://allthingsd.com/20050714/tracking-cookies/ ("Suppose you bought a TV set that included a component to track what you watched, and then reported that data back to a company that used or sold it for advertising purposes. Only nobody told you the tracking technology was there or asked your permission to use it. You would likely be outraged at this violation of privacy. Yet that kind of Big Brother intrusion goes on everyday on the Internet . . . [with tracking cookies].").

35 *See In re Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcompt.pdf.

36 *See In re Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

37 Although the complaint against Google alleged that the company used deceptive tactics and violated its own privacy promises when it launched Google Buzz, even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm. *See* Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm (noting that in response to the Buzz launch, Google received thousands of complaints from consumers who were concerned about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers, or competitors).

38 *See, e.g.*, Statement of John M. Montgomery, GroupM Interaction, *The State of Online Consumer Privacy*: *Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 112th Cong. (Mar. 16, 2011), *available at* http://www.iab.net/media/file/DC1DOCS1-432016-v1-John_Montgomery_-_Written_Testimony.pdf ("We at GroupM strongly believe in protecting consumer privacy. It is not only the right thing to do, but it is also good for business."); Statement of Alan Davidson, Director of Public Policy, Google Inc., *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the S. Subcomm. on Privacy, Tech., and the Law*, 112th Cong. (May 10, 2011), *available at* http://www.judiciary.senate.gov/pdf/11-5-10%20Davidson%20Testimony.pdf ("Protecting privacy and security is essential for Internet commerce.").

example, in the online behavioral advertising area, a recent survey shows that consumers feel better about brands that give them transparency and control over advertisements.[39]

Companies offering consumers information about behavioral advertising and the tools to opt out of it have also found increased customer engagement. In its comment, Google noted that visitors to its Ads Preference Manager are far more likely to edit their interest settings and remain opted in rather than to opt out.[40] Similarly, another commenter conducted a study showing that making its customers aware of its privacy and data security principles – including restricting the sharing of customer data, increasing the transparency of data practices, and providing access to the consumer data it maintains – significantly increased customer trust in its company.[41]

In addition, some companies appear to be competing on privacy. For example, one company offers an Internet search service that it promotes as being far more privacy-sensitive than other search engines.[42] Similarly, in response to Google's decision to change its privacy policies to allow tracking of consumers across different Google products, Microsoft encouraged consumers to switch to Microsoft's more privacy-protective products and services.[43]

The privacy framework is designed to be flexible to permit and encourage innovation. Companies can implement the privacy protections of the framework in a way that is proportional to the nature, sensitivity, and amount of data collected as well as to the size of the business at issue. For example, the framework does not include rigid provisions such as specific disclosures or mandatory data retention and destruction periods. And, as discussed below, the framework streamlines communications for businesses and consumers alike by requiring consumer choice mechanisms only for data practices that are inconsistent with the context of a particular transaction or the business relationship with the consumer.[44]

B. GLOBAL INTEROPERABILITY

Reflecting differing legal, policy, and constitutional regimes, privacy frameworks around the world vary considerably. Many commenters cited the value to both consumers and businesses of promoting more consistent and interoperable approaches to protecting consumer privacy internationally. These commenters stated that consistency between different privacy regimes reduces companies' costs, promotes international competitiveness, and increases compliance with privacy standards.[45]

39 *See RESEARCH: Consumers Feel Better About Brands That Give Them Transparency and Control Over Ads*, Evidon Blog (Nov. 10, 2010), http://blog.evidon.com/tag/better-advertising ("when advertisers empower consumers with information and control over the ads they receive, a majority feels more positive toward those brands, and 36% even become more likely to purchase from those brands").

40 *See Comment of Google Inc.*, cmt. #00417, at 4.

41 *See Comment of Intuit, Inc.*, cmt. #00348, at 6-8 ("The more transparent (meaning open, simple and clear) the company is, the more customer trust increases. . . .").

42 *See* DuckDuckGo, Privacy Policy, https://duckduckgo.com/privacy.html.

43 *See* Frank X. Shaw, *Gone Google? Got Concerns? We Have Alternatives*, The Official Microsoft Blog (Feb. 1, 2012, 2:00 AM), http://blogs.technet.com/b/microsoft_blog/archive/2012/02/01/gone-google-got-concerns-we-have-alternatives.aspx.

44 See *infra* at Section IV.C.1.a.

45 *See Comment of AT&T Inc.*, cmt. #00420, at 12-13; *Comment of IBM*, cmt. #00433, at 2; *see also Comment of General Electric*, cmt. #00392, at 3 (encouraging international harmonization).

The Commission agrees there is value in greater interoperability among data privacy regimes as consumer data is increasingly transferred around the world. Meaningful protection for such data requires convergence on core principles, an ability of legal regimes to work together, and enhanced cross-border enforcement cooperation. Such interoperability is better for consumers, whose data will be subject to more consistent protection wherever it travels, and more efficient for businesses by reducing the burdens of compliance with differing, and sometimes conflicting, rules. In short, as the Administration White Paper notes, global interoperability "will provide more consistent protections for consumers and lower compliance burdens for companies."[46]

Efforts underway around the world to re-examine current approaches to protecting consumer privacy indicate an interest in convergence on overarching principles and a desire to develop greater interoperability. For example, the Commission's privacy framework is consistent with the nine privacy principles set forth in the 2004 Asia-Pacific Economic Cooperation ("APEC") Privacy Framework. Those principles form the basis for ongoing APEC work to implement a cross-border privacy rules system to facilitate data transfers among the 21 APEC member economies, including the United States.[47] In 2011, the Organization for Economic Cooperation and Development ("OECD") issued a report re-examining its seminal 1980 Privacy Guidelines in light of technological changes over the past thirty years.[48] Further, the European Commission has recently proposed legislation updating its 1995 data protection directive and proposed an overhaul of the European Union approach that focuses on many of the issues raised elsewhere in this report as well as issues relating to international transfers and interoperability.[49] These efforts reflect a commitment to many of the high-level principles embodied in the FTC's framework – increased transparency and consumer control, the need for privacy protections to be built into basic business practices, and the importance of accountability and enforcement. They also reflect a shared international interest in having systems that work better with each other, and are thus better for consumers.

46 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, ii, Foreword (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

47 The nine principles in the APEC Privacy Framework are preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, accountability. Businesses have developed a code of conduct based on these nine principles and will obtain third-party certification of their compliance. A network of privacy enforcement authorities from participating APEC economies, such as the FTC, will be able to take enforcement actions against companies that violate their commitments under the code of conduct. *See* Press Release, FTC, FTC Welcomes a New Privacy System for the Movement of Consumer Data Between the United States and Other Economies in the Asia-Pacific Region (Nov. 14, 2011), *available at* http://www.ftc.gov/opa/2011/11/apec.shtm).

48 *See* Organization for Economic Co-operation and Development, *The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines* (Apr. 2011), *available at* http://www.oecd.org/dataoecd/22/25/47683378.pdf.

49 European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

C. LEGISLATION TO AUGMENT SELF-REGULATORY EFFORTS

Numerous comments, including those from large industry stakeholders, consumer and privacy advocates, and individual consumers supported some form of baseline privacy legislation that incorporates the FIPPs.[50] Business commenters noted that legislation would help provide legal certainty,[51] serve as a key mechanism for building trust among customers,[52] and provide a way to fill gaps in existing sector-based laws.[53] Consumer and privacy advocates cited the inability of self-regulation to provide comprehensive and long-lasting protection for consumers.[54] One such commenter cited the fact that many self-regulatory initiatives that arose in response to the Commission's 2000 recommendation for privacy legislation were short-lived and failed to provide long-term privacy protections for consumers.[55]

At the same time, a number of commenters raised concerns about government action beyond providing guidance for self-regulatory programs.[56] Some cautioned the FTC about taking an approach that might impede industry's ability to innovate and develop new products and services in a rapidly changing marketplace. Others noted that a regulatory approach could lead to picking "winners and losers" among particular technologies and business models and called for a technology-neutral approach.[57] Commenters also argued that it might be impractical to craft omnibus standards or rules that would apply broadly across different business sectors.[58]

The Commission agrees that, to date, self-regulation has not gone far enough. In most areas, with the notable exception of efforts surrounding Do Not Track, there has been little self-regulation. For example, the FTC's recent survey of mobile apps marketed to children revealed that many of these apps fail to provide any disclosure about the extent to which they collect and share consumers' personal data.[59] Similarly, efforts

50 *See, e.g.*, *Comment of eBay*, cmt. #00374, at 2; *Comment of Intel Corp.*, cmt. #00246, at 3-7; *Comment of Microsoft Corp.*, cmt. #00395, at 4; *Comment of Intuit, Inc.*, cmt. #00348, at 13-14; *Comment of Center for Democracy & Technology*, cmt. #00469, at 1, 7; *Comment of Gregory Byrd*, cmt. #00144, at 1; *Comment of Ellen Klinefelter*, cmt. #00095, at 1.

51 *See Comment of Microsoft Corp.*, cmt. #00395, at 4.

52 *See Comment of Intel Corp.*, cmt. #00246, at 3.

53 *See Comment of Intuit, Inc.*, cmt. #00348, at 13.

54 *See Comment of Electronic Privacy Information Center*, cmt. #00386, at 2; *Comment of World Privacy Forum*, cmt. #00376, at 2-3, 8-17.

55 *See Comment of World Privacy Forum*, cmt. #00376, at 2-3, 8-17.

56 *See Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4-5; *Comment of American Catalog Mailers Ass'n*, cmt. #00424, at 3; *Comment of Facebook, Inc.*, cmt. #00413, at 13-14; *Comment of Google Inc.*, cmt. #00417, at 8; *Comment of Verizon*, cmt. #00428, at 2-3, 6-7, 14-17; *Comment of Mortgage Bankers Ass'n*, cmt. #00308, at 2; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 3, 5, 7-13; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 15.

57 *See Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 32-37; *Comment of USTelecom*, cmt. #00411, at 5-7; *Comment of Verizon*, cmt. #00428, at 4-6; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 5-6.

58 *See Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4-6; *see also Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 8-11; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 13.

59 FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; *FPF Finds Nearly Three-Quarters of Most Downloaded Mobile Apps Lack a Privacy Policy*, Future of Privacy Forum, http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/.

of the data broker industry to establish self-regulatory rules concerning consumer privacy have fallen short.[60] These examples illustrate that even in some well-established markets, basic privacy concepts like transparency about the nature of companies' data practices and meaningful consumer control are absent. This absence erodes consumer trust.

There is also widespread evidence of data breaches and vulnerabilities related to consumer information.[61] Published reports indicate that some breaches may have resulted from the unintentional release of consumer data, for which companies later apologized and took action to address.[62] Other incidents involved planned releases or uses of data by companies that ultimately did not occur due to consumer and public backlash.[63] Still other incidents involved companies' failure to take reasonable precautions and resulted in FTC consent decrees. These incidents further undermine consumer trust, which is essential for business growth and innovation.[64]

The ongoing and widespread incidents of unauthorized or improper use and sharing of personal information are evidence of two points. First, companies that do not intend to undermine consumer privacy simply lack sufficiently clear standards to operate and innovate while respecting the expectations of consumers. Second, companies that do seek to cut corners on consumer privacy do not have adequate legal incentives to curtail such behavior.

To provide clear standards and appropriate incentives to ensure basic privacy protections across all industry sectors, in addition to reiterating its call for federal data security legislation,[65] the Commission calls

60 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 2-3; *Comment of World Privacy Forum*, cmt. #00376, at 2-3. Discussed more fully *infra* at Section IV.D.2.a.

61 *See* Grant Gross, *Lawmakers Question Sony, Epsilon on Data Breaches,* PC World (June 2, 2011 3:40 PM), *available at* http://www.pcworld.com/businesscenter/article/229258/lawmakers_question_sony_epsilon_on_data_breaches.html; Dwight Silverman, *App Privacy: Who's Uploading Your Contact List?*, Houston Chronicle (Feb. 15, 2012 8:10 AM), http://blog.chron.com/techblog/2012/02/app-privacy-whos-uploading-your-contact-list/; Dan Graziano, *Like iOS apps, Android Apps Can Secretly Access Photos Thanks to Loophole,* BGR (Mar. 1, 2012 3:45 PM), http://www.bgr.com/2012/03/01/like-ios-apps-android-apps-can-also-secretly-access-photos-thanks-to-security-hole/.

62 *CEO Apologizes After Path Social App Uploads Contact Lists,* KMOV.com (Feb. 9, 2012 11:11AM), http://www.kmov.com/news/consumer/CEO-apologizes-after-Path-uploads-contact-lists--139015729.html; Daisuke Wakabayashi, *A Contrite Sony Vows Tighter Security,* Wall St. J. May 1, 2011, *available at* http://online.wsj.com/article/SB10001424052748704436004576296302384608280.html.

63 Kevin Parrish, *OnStar Changes its Mind About Tracking Vehicles,* Tom's Guide (Sept. 29, 2011 7:30 AM), http://www.tomsguide.com/us/OnStar-General-motors-Linda-Marshall-GPS-Terms-and-conditions,news-12677.html.

64 Surveys of consumer attitudes towards privacy conducted in the past year are illuminating. For example, a *USA Today*/Gallup poll indicated that a majority of the Facebook members or Google users surveyed were "very" or "somewhat concerned" about their privacy while using these services. Lymari Morales, *Google and Facebook Users Skew Young, Affluent, and Educated*, Gallup (Feb. 17, 2011), *available at* http://www.gallup.com/poll/146159/facebook-google-users-skew-young-affluent-educated.aspx.

65 The Commission has long supported federal laws requiring companies to implement reasonable security measures and to notify consumers in the event of certain security breaches. *See, e.g.*, Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft*: *Hearing Before the Before the H. Comm. on Ways and Means, Subcomm. on Social Security*, 112th Cong. (April 13, 2011), *available at* http://www.ftc.gov/os/testimony/110411ssn-idtheft.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf.

on Congress to consider enacting baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate. The Commission is prepared to work with Congress and other stakeholders to craft such legislation.

In their comments, many businesses indicated that they already incorporate the FIPPS into their practices. For these companies, a legislative mandate should not impose an undue burden and indeed, will "level the playing field" by ensuring that all companies are required to incorporate these principles into their practices.

For those companies that are not already taking consumer privacy into account – either because of lack of understanding or lack of concern – legislation should provide clear rules of the road. It should also provide adequate deterrence through the availability of civil penalties and other remedies.[66] In short, legislation will provide businesses with the certainty they need to understand their obligations and the incentive to meet those obligations, while providing consumers with confidence that businesses will be required to respect their privacy. This approach will create an environment that allows businesses to continue to innovate and consumers to embrace those innovations without sacrificing their privacy.[67] The Commission is prepared to work with Congress and other stakeholders to formulate baseline privacy legislation.

While Congress considers such legislation, the Commission urges industry to accelerate the pace of its self-regulatory measures to implement the Commission's final privacy framework. Over the course of the next year, Commission staff will promote the framework's implementation by focusing its policymaking efforts on five main action items, which are highlighted here and discussed further throughout the report.

- **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.
- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures.[68] As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to

66 Former FTC Chairman Casper "Cap" Weinberger recognized the value of civil penalties as a deterrent to unlawful conduct. *See Hearings on H.R. 14931 and Related Bills before the Subcomm. on Commerce and Finance of the H. Comm. on Interstate and Foreign Commerce*, 91st Cong. 53, 54 (1970) (statement of FTC Chairman Caspar Weinberger); *Hearings on S. 2246, S. 3092, and S. 3201 Before the Consumer Subcomm. of the S. Comm. on Commerce*, 91st Cong. 9 (1970) (Letter from FTC Chairman Caspar W. Weinberger) (forwarding copy of House testimony).

67 With this report, the Commission is not seeking to impose civil penalties for privacy violations under the FTC Act. Rather, in the event Congress enacts privacy legislation, the Commission believes that such legislation would be more effective if the FTC were authorized to obtain civil penalties for violations.

68 *See* Press Release, FTC, FTC Seeks Input to Revising its Guidance to Businesses About Disclosures in Online Advertising (May 26, 2011), *available at* http://www.ftc.gov/opa/2011/05/dotcom.shtm.

consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

- **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker.[69] To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers ("ISPs"), operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.
- **Promoting enforceable self-regulatory codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

69 *See* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011).