A MARRIAGE OF CONVENIENCE? A COMMENT ON *THE PROTECTION OF DATABASES*

JANE C. GINSBURG*

INTRODUCTION

Daniel Gervais concluded his analysis of the protection of databases with three options for the future.[1] I would like to examine a fourth. Let us assume no future flurry of national or supranational legislative activity because the content of databases is in fact already being protected. Not through copyright or *sui generis* rights, but through other means. Databases are an object of economic value, and they will conveniently wed whatever legal theory or theories will achieve the practical objective of preventing unauthorized exploitation of the works' contents. To beat the marriage metaphor into the ground, I'd like to suggest that, at least in the U.S., databases today can avail themselves of the traditional range of wedding gifts: "something old, something new, something borrowed, something blue."

The something old is contract law; the something new is the Computer Fraud and Abuse Act;[2] the something borrowed is the newly reminted tort of "trespass to chattels";[3] and the something blue—using "blue" in the sense of something risqué and perhaps objectionable—is digital rights management, reinforced by the anti-circumvention protections of § 1201 of the Digital Millennium Copyright Act.[4]

I. SOMETHING OLD

Contracts have served to secure valuable information long before the digital era. Financial information, "hot news," and such have been the ob-

* Morton L. Janklow Professor of Literary and Artistic Property Law, Columbia University School of Law. Thanks for research assistance to Margaret Ciavarella, Columbia Law School class of 2007.

[1] Daniel J. Gervais, *The Protection of Databases*, 82 CHI.-KENT L. REV. 1109 (2007).

[2] 18 U.S.C. § 1030 (2000).

[3] *See, e.g.*, Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 404–05 (2d Cir. 2004); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1069–73 (N.D. Cal. 2000).

[4] 17 U.S.C. § 1201 (2000).

ject of subscription contracts.[5] Courts have upheld the subscribers' contractually incurred obligations not to disclose the information to third parties, even though the information did not benefit from copyright protection.[6] With digitization of the information and development of standard, mass-market contracts, courts have continued to uphold the contracts' restrictions on reuse of the information,[7] even though the shrink-wrap—and especially the click-wrap or browse-wrap—nature of those "agreements" significantly erode the distinction between *inter-partes* contract rights and *erga-omnes* property rights. I will not elaborate further on contracts as a means of creating *de facto* intellectual property rights, because that is the topic of Séverine Dusollier's paper for a later panel of this conference.[8]

II. SOMETHING NEW

The Computer Fraud and Abuse Act ("CFAA") creates civil and criminal liability for one who "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 . . . ."[9] As a threshold standing requirement, the claimant must have sustained an aggregate loss of at least $5,000 in the course of a year.[10] A "protected computer" under the CFAA is any computer used in "interstate or foreign commerce or communication," which in effect includes virtually all computers in commercial use, for example, any computer connected to the Internet. The two sections of the CFAA most relevant to database protection are § 1030(a)(2)(C), which prohibits intentionally accessing without authorization or exceeding authorized access to a computer, and thus obtaining information from a protected computer; and § 1030(a)(5)(C), which prohibits intentionally accessing a protected com-

[5] *See, e.g.*, Bd. of Trade v. Christie Grain & Stock Co., 198 U.S. 236 (1905) (confidential grain price quotations); F.W. Dodge Co. v. Constr. Info. Co., 66 N.E. 204 (Mass. 1903) (reports of building construction information); Exch. Tel. Co. Ltd. v. Gregory & Co., [1896] 1 Q.B. 147 (C.A.) (financial information disclosed to subscribers); *see also* Ladd v. Oxnard, 75 F. 703 (C.C.D. Mass. 1896) (credit ratings of stone dealers; restricted circulation kept work within common law copyright).

[6] *See, e.g.*, *F.W. Dodge*, 66 N.E. at 206. Courts have also upheld trade secret protection for confidential sales and business information. *See, e.g.*, RKI, Inc. v. Grimes, 177 F. Supp. 2d 859 (N.D. Ill. 2001) (proprietary system listing customer and sales information); NewInno, Inc. v. Peregrim Dev., Inc., No. CV010390074S, 2002 Conn. Super. LEXIS 3907 (Conn. Super. Ct. Nov. 27, 2002) (system tying expert consultants to customers and containing data on each).

[7] *See*, *e.g.*, Wall Data Inc. v. L.A. County Sheriff's Dep't, 447 F.3d 769, 774 (9th Cir. 2006); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996).

[8] Séverine Dusollier, *Sharing Access to Intellectual Property Through Private Ordering*, 82 CHI.-KENT L. REV. 1391 (2007).

[9] 18 U.S.C. § 1030(a)(4) (2000).

[10] *Id.*; *see also* Register.com, Inc. v. Verio, Inc., 356 F.3d 393 app. at 439–40 (2d Cir. 2004) (Parker, J., draft opinion).

puter without authorization, and as a result of such conduct, causing damage or loss. Courts have interpreted "unauthorized access" broadly. The First Circuit, for instance, has held that "[a] lack of authorization could be established by an explicit statement on the website restricting access."[11] In other examples, database producers have successfully pleaded CFAA claims in cases involving the "scraping" of pricing information from a tour operator's database[12] and the copying of market data reports.[13] CFAA claims may be particularly useful against competitors who systematically copy frequently updated information from a "dynamic" database.

III. SOMETHING BORROWED

The old wine in a new bottle, or—consistent with our opening metaphor—the old legal theory recycled with new gift-wrapping, is the common law action of "trespass to chattels." At common law, a defendant commits trespass to chattels when he intentionally either "dispossess[es] another of the chattel" or "us[es] or intermeddl[es] with a chattel in the possession of another."[14] Liability for intermeddling attaches 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, . . . or . . . harm is caused to some person or thing in which the possessor has a legally protected interest."[15] The tort made its computer-age debut in *Thrifty-Tel, Inc. v. Bezenek*. There, a group of teenagers obtained a secret access code to a long distance telephone company and repeatedly dialed into its network in an endeavor to make free long-distance calls. Although they failed, their insistent attempts tied up a substantial portion of the telephone network. The court ruled that the electronic signals forming the network constituted the chattel with which the teenagers interfered, and held them liable for trespass to chattels.[16]

The first use of the tort specifically in the Internet context occurred in *CompuServe, Inc. v. Cyber Promotions, Inc*. There, the court found trespass to chattels when the defendant sent large quantities of spam to Compu-

[11] EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003).

[12] *Id.* at 63; EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).

[13] I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 524–26 (S.D.N.Y. 2004). *See generally* James A. Tanner, *How Much Protection Is Too Much: Using the Computer Fraud and Abuse Act as an Appropriate Means to Protect Compilations of Data*, SYRACUSE SCI. & TECH. L. REP., Spring 2004, http://www.law.syr.edu/students/publications/sstlr/framesets/archive/archived/spring04/James.pdf.

[14] RESTATEMENT (SECOND) OF TORTS § 217 (1965).

[15] *Id.* § 218(b)–(d).

[16] 54 Cal. Rptr. 2d 468, 472–73 (Cal. Ct. App. 1996).

Serve's customers. The volume of the emails burdened and slowed down CompuServe's networks, and many customers, frustrated by receiving spam, discontinued their CompuServe subscriptions.[17] Other courts have adapted the trespass to chattels action to redress network operators' complaints of "spamming."[18]

In 2000, the Northern District of California, in *eBay, Inc. v. Bidder's Edge, Inc.*, significantly expanded the concept of "harm" in cyberspace trespass to chattels claims. Bidder's Edge was an auction aggregation service that used "spidering" technology—a high-powered automated search method enabling continuous updating of large quantities of data—to gather data from auction websites such as eBay, so that consumers could compare the price of a given item across online auction sites. Despite eBay's objection to Bidder's Edge's data collection, Bidder's Edge continued to spider eBay's site. In the ensuing lawsuit, eBay prevailed on its trespass to chattels claim, even though it could not show actual harm to its website—such as slow or impaired functioning—or lost customers, as the spamming claimants had. The court reasoned that allowing Bidder's Edge to spider would encourage other auction aggregators to do so as well, and this combined effect would be likely to harm the performance of eBay's computer system.[19]

Despite widespread concern among legal scholars that extension of the trespass to chattel tort to situations in which no actual damage can be shown will lead to suboptimal use of Internet resources,[20] courts in other

[17] 962 F. Supp. 1015 (S.D. Ohio 1997).

[18] *See, e.g.*, America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998) (holding that unsolicited bulk email constituted trespass to chattels); America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998) (same).

[19] 100 F. Supp. 2d 1058, 1069–73 (N.D. Cal. 2000).

[20] *See, e.g.*, Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 39–54 (2000) (arguing that application of trespass to chattels to digital environment is inappropriate and dangerous); Edward W. Chang, *Bidding on Trespass:* eBay, Inc. v. Bidder's Edge, Inc. *and the Abuse of Trespass Theory in Cyberspace Law*, 29 AIPLA Q.J. 445 (2001) (predicting that application of the *eBay* holding will chill use of Internet databases); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 500–18 (2003) (arguing that overexpansion of Internet property rights will destroy Internet's value as a common resource). *But see* Daniel Kearney, *Network Effects and the Emerging Doctrine of Cybertrespass*, 23 YALE L. & POL'Y REV. 313 (2005) (proposing possible benefits and positive incentives to the public from current cybertrespass doctrine).

Commentators also object to the adaptation to computer networks of a tort conceived to protect tangible property. *See, e.g.*, Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421, 438 (2002) (arguing that "[t]he trespass to chattels doctrine, designed to ensure that a single, indivisible piece of tangible property is available to its owner" is difficult to apply to a "chattel" whose entire purpose is to be part of a network accessible to and used by others); Burk, *supra*, at 33–34 (citing W. PAGE KEETON ET AL., PROSSER & KEETON ON THE LAW OF TORTS § 13, at 71 (5th ed. 1984)). Burk argues that the current line of trespass to chattels cases has ignored the tort's roots as "the little brother of conversion." Both torts are intended to remedy the "dispossession" of a chattel; conversion is total dispossession and trespass to chattels is partial disposjurisdictions have adopted *eBay*'s approach. For example, in *Register.com, Inc. v. Verio, Inc.*, the Second Circuit upheld the district court's denial of a motion to dismiss a trespass to chattels claim where Verio used a search robot—a software program which performs multiple automated queries—to search the database of Internet domain names on the plaintiff's website. The court followed the same slippery slope reasoning as the *eBay* court, stating that allowing one ISP to use a search robot on the site would most likely lead others to do so as well and collectively overtax Register.com's computer system.[21]

While some courts have placed limits on Internet-related trespass to chattels claims where little or no actual damage to the plaintiff's computer system can be shown,[22] decisions like *eBay* and its progeny still offer a formidable arm to database proprietors who seek to prevent the extraction of information from their electronic databases. Among database proprietors, the greatest beneficiaries of trespass to chattels claims are likely to be the larger and more commercially important dynamic databases, for these are the types of databases for which an effective search may well require robots or other such technologies.

IV. SOMETHING BLUE[23]

Finally, among extra-copyright means of protecting databases, resort to legally-secured technological protection measures may be the most controversial. It may also enjoy broader use than some of the other "wedding gifts," because the protection attaches to the collection of data, not to a computer network through which the data might be accessed. A database producer could always distribute the product with an access- or copy-

session. But in finding that an owner has been "dispossessed" of her moving electrons when other electrons pass through them just as they are designed to, courts are effectively striking out the term "dispossess" and redefining the tort as a rule of inviolability. This is the standard associated with trespass to *land*, not chattels. *Id.*

[21] 356 F.3d 393, 404 (2d Cir. 2004).

[22] *See, e.g.*, Ticketmaster Corp. v. Tickets.com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003) (dismissing trespass to chattels claim because defendant's use of search robots only caused negligible harm to plaintiff); *see also* Intel Corp. v. Hamidi, 71 P.3d 296, 302–11 (Cal. 2003) (refusing to hold that six mass emails to Intel employees are a sufficient burden on Intel's computer system to sustain trespass to chattels claim). *But see* Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724 JCS, 2001 WL 1736382, at **11–13 (N.D. Cal. Dec. 6, 2001) (declining to follow *Ticketmaster*'s requirement of "more than negligible" harm to plaintiff to sustain trespass to chattels claim). *Oyster Software* was also a search robot case.

[23] This section is adapted from Jane C. Ginsburg, *U.S. Initiatives to Protect Works of Low Authorship*, *in* EXPANDING THE BOUNDARIES OF INTELLECTUAL PROPERTY: INNOVATION POLICY FOR THE KNOWLEDGE SOCIETY 55 (Rochelle Cooper Dreyfuss et al. eds., 2001).

control, but until the 1998 Digital Millennium Copyright Act ("DMCA"),[24] others were probably free to hack those controls, either directly or through a generally distributed circumvention device. The DMCA added § 1201 to the Copyright Act; that provision defined three new violations: First, § 1201(a)(1) prohibits circumvention of technological protection measures that control "access" to copyrighted works. Second, § 1201(a)(2) makes it a violation to manufacture, disseminate, offer, etc. devices, services, etc. that circumvent access controls. Finally, § 1201(b) makes it a violation to manufacture, disseminate, offer, etc. devices or services, etc. that circumvent a technological measure that "effectively protects a right of the copyright owner . . . ."[25] While these provisions address protection of copyrighted works, a database producer who password-protects, encrypts, or otherwise technologically protects the contents of a minimally original compilation might be able to rely on § 1201 to insulate those contents from copying, even if the material sought to be reproduced is not copyrightable.

Although § 1201(a) governs "a work protected under this title," it does not specify how *much* of the work must be protected, nor does it distinguish "thin copyright" works from more creative endeavors. As a result, to benefit from § 1201(a), it appears that so long as a database producer does not merely encrypt raw public domain documents or unoriginal listings of information, but instead packages the information with copyrightable trappings—such as a new introduction, or minimally original reformatting[26]—the database would be a copyrighted work, however scant the covering. This suggests that the copyrightable "fig leaf" a database producer affixes to an otherwise unprotectable work could, as a practical matter, obscure the public domain nakedness of the compiled information.

Section 1201 does include a variety of exceptions to the prohibition on access circumvention, but these are extremely specific, and none directly apply to databases.[27] Worse, the extraordinarily narrow drafting of the exceptions discourages attempts to discern from them an overall legislative policy regarding the kinds of circumventions that should offset copyright owners' enhanced ability to control access to their works. Indeed, if anything, the proliferation of special case exceptions, and Congress's delega-

[24] Pub. L. No. 105-304, §§ 103, 202, 112 Stat. 2860, 2863–76, 2877–86 (1998) (adding §§ 1201–1203 and § 512 to the Copyright Act of 1976).

[25] 17 U.S.C. § 1201(a)–(b) (2000).

[26] *See, e.g.*, Maljack Prods., Inc. v. UAV Corp., 964 F. Supp. 1416, 1426–29 (C.D. Cal. 1997) (holding that "panning and scanning" modifications to a film in the public domain are copyrightable), *aff'd on other grounds sub nom.*, Batjack Prods., Inc. v. GoodTimes Home Video Corp., 160 F.3d 1223 (9th Cir. 1998).

[27] *See* 17 U.S.C. § 1201(d)–(j).

tion to the Copyright Office to make triennial rulings exempting certain classes of works,[28] prompt the negative inference that any access circumvention not expressly legislatively or administratively exempted is prohibited.[29]

Arguably, § 1201(c) accords courts residual authority to expand exceptions to access control. That provision specifies that nothing in § 1201 affects "defenses to copyright infringement, including fair use, under this title."[30] But a violation of § 1201(a) is not copyright infringement; it is a new violation for which the DMCA provides distinct remedies.[31] Nonetheless, circumvention claims remain copyright dependent, since § 1201 covers only measures that protect access to copyrighted works. Perhaps, were a court persuaded that the challenged act of circumvention (or use of an access-circumvention device) would not under the circumstances lead to copyright infringement, because—as in the case of a copyrightable "fig leaf" covering a collection of public domain information—whatever access to a copyrighted work the act or device permits is incidental and necessary to access unprotected data, then the circumvention might be excused.[32]

RETURNING THE GIFTS TO THE STORE

Ultimately, indirect approaches to database protection, such as those discussed here, cannot provide a comprehensive response to the problems of either the under- or overprotection of databases. Not all non-original databases will benefit from a quasi-property regime derived from claims of interference with computer networks. Notably, if the database proprietor is not also the computer network operator, those claims would not seem to apply. By the same token, the CFAA would not assist modest proprietors; it

[28] *See id.* § 1201(a)(1)(B)–(D).

[29] *See, e.g.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429, 443 n.13 (2d Cir. 2001).

[30] 17 U.S.C. § 1201(c)(1).

[31] *See id.* § 1203. Remedies for copyright infringement are set forth at *id.* §§ 502–510.

[32] *Cf.* Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307, 1311–19 (Fed. Cir. 2005) (holding that circumvention of the code controlling access to data library maintenance software did not violate § 1201 because access did not "facilitate copyright infringement"; copies made in RAM once the software was accessed were copies permitted under the § 117(c) exception for computer maintenance); Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1197–1203 (Fed. Cir. 2004) (involving the circumvention of computer code controlling access to a garage door; the court interpolated into § 1201 a requirement that the protection against circumvention of an access control be related to protection against infringement).

That said, however, one must recognize that not all databases that § 1201(a) might otherwise overprotect are plainly of the "fig leaf" variety. It will not always be easy to distinguish the pretextual copyrightable "fig leaf" from a substantial authorship contribution. For example, the copyrightable work incorporating public domain information might be a compilation or collective work containing both copyrightable and public domain elements.

does not redress appropriations that do not cause over $5,000 in aggregate annual loss. Moreover, bootstrapping database protection to technological protection measures is not likely to install a sensible intellectual property regime, whether from the point of view of information providers or users. Keeping in mind the dangers of *sui generis* legislation (whose pitfalls in the E.U. Daniel Gervais has documented) it might nonetheless be preferable to devise a statute attentive to both users and proprietors, and carefully tailored to ensure meaningful incentives to gather, organize, and disseminate information, without unduly encumbering research and derivative uses of the collected information.