NEW THEORIES OF DATABASE PROTECTION

Jonathan Band

In 1991, the U.S. Supreme Court in *Feist Publications v. Rural Telephone*, 499 U.S. 340 (1991), rejected the "sweat of the brow" doctrine that bestowed copyright protection on the facts contained in databases by virtue of the effort the publisher expended in collecting the facts. Instead, the Supreme Court made clear that the Constitution's Intellectual Property Clause permitted copyright to protect only the original expression reflected by the selection, coordination, and arrangement of the facts. The facts themselves remained in the public domain, free for others to copy and distribute.

In the years since *Feist*, particularly after the EU adopted its Database Directive in 1996, some database publishers have lobbied Congress to adopt legislation extending additional intellectual property protection for databases. Because of extensive opposition from the financial services, Internet, library, and university communities, Congress has not adopted *sui generis* database legislation. In the meantime, however, courts have extended state common law trespass to chattels and the federal Computer Fraud and Abuse Act (CFAA) to online databases. As applied by some courts, these legal doctrines provide a supercharged surrogate copyright protection to the facts contained in publicly available online databases. These doctrines thus provide database publishers the kind of protection found unconstitutional by the Supreme Court in *Feist*, and granted by the EU Database Directive. Accordingly, these doctrines obviate the need for additional database legislation in the U.S.

This article will examine this recent trend. First, the article will discuss judicial decisions that apply trespass to chattels to online databases. Next, the article will review the decisions that have found liability under the CFAA for the extraction of facts from publicly accessible websites. Finally, the article will assess whether the Constitution limits this extension of trespass to chattels and the CFAA. This article will not address the more well established forms of database protection, including copyright, contract, common law misappropriation, and technological measures.

Trespass To Chattels

The state common law cause of action for trespass to chattels refers to an act of intentional interference with the possessory rights of another's personal property. To prevail, the plaintiff must show (1) that the defendant intentionally interfered without authorization with the plaintiff's possessory rights in personal property, and that (2) the unauthorized use by the defendant resulted in damage to the plaintiff. This ancient English common law doctrine was first applied to cyberspace in spam cases, where Internet service providers were searching for a legal mechanism to stop marketers from flooding their systems with literally millions of unsolicited commercial emails. More recently, publishers of publicly accessible online databases have employed trespass to chattel claims against competitors who accessed the databases and extracted facts.

So far, four U.S. courts have considered the trespass to chattels theory in cases involving the extraction of facts from websites by search robots. In three of these cases, the courts granted either preliminary or final relief to the complaining website operator. In only one case the court rejected the application of the trespass theory.

The first and perhaps best known case is ***eBay v. Bidder's Edge***, 100 F. Supp.2d 1058 (N.D. Ca. 2000). BE was an "auction aggregator" that combined the auction listings from numerous online auction sites, including eBay, so that a user could go to one site to see what was available on all sites, rather than making separate visits to each auction site. To obtain the auction listings from eBay and the other auction sites, BE used software "web crawlers" that made multiple queries of the eBay auction database – sometimes as many as 100,000 times per day.

BE argued that it could not trespass upon eBay's site because the eBay site is publicly accessible. The court ruled that eBay granted only conditional access to its site, and that BE grossly exceeded those conditions by making repeated queries. Additionally, BE ignored eBay's specific requests that it stop its web crawling.

The court next considered whether BE's use of the eBay website caused damage. eBay claimed that BE's queries consumed valuable bandwidth and server capacity, "necessarily compromising eBay's ability to use that capacity for its own purposes." BE responded that its searches represented a negligible load on eBay's system, using less than 2% of eBay's capacity. The court ruled that "[e]ven if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes." The court held that the mere interference with a possessory interest is sufficient to establish damage.

At the same time, the court appeared uncomfortable with its finding that BE's mere use of the site causes injury. Thus, the court speculated that about the injury that might result if it did not stop BE: "If the court were to hold otherwise, it would likely

encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If…other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value." Therefore, the court implicitly acknowledged that BE actually did not cause eBay any harm, but that eBay would be harmed if many aggregators behaved in the same manner as BE.

The court in *Register.com v. Verio,* 126 F.Supp. 2d 238 (S.D.N.Y.) relied heavily on *eBay* in ruling that Verio's extraction of facts from Register.com's WHOIS database constituted a trespass to chattels. The court in *Oyster Software v. Forms Processing,* 2001 U.S. Dist. LEXIS 22520 (N.D. Cal. 2001) likewise agreed with the *eBay* court's ruling that simple use of the plaintiff's computer was sufficient to establish damage and that no showing of physical harm or substantial interference was necessary. Accordingly, the *Oyster* court found liability even though "Oyster has presented no evidence that the use of Top-Ten's robot interfered with the basic function of Oyster's computer system" and "Oyster concedes that Top-Ten's robot placed a 'negligible' load on Oyster's computer system."

As noted, the *eBay* court suggested that it based its holding that mere use equals damage at least in part on the actual harm the plaintiffs would suffer if other entities acted in the same manner as the defendants. The *Oyster* court dispensed with this speculative justification. The plaintiff only needed to show unauthorized use of its website in order to prevail on a trespass to chattels claim.

The sole dissenting view appeared in the decision in *Ticketmaster Corp. v. Tickets.com*, 2000 U.S. Dist. LEXIS 12987 (C.D. Ca. 2000), a case involving the

extraction of concert information from the Ticketmaster website. After discussing the *eBay* decision, the *Ticketmaster* court appeared to reject the *eBay* court's holding that mere possessory interference constitutes sufficient harm for trespass to chattels liability. Instead, the court stated that "[a] basic element of trespass to chattels must be physical harm to the chattel … or some obstruction of its basic function …." The court seemed to acknowledge that many companies simultaneously extracting information from a website could have the cumulative effect of interfering with the website's operation. However, unlike the *eBay* court, the *Ticketmaster* court was not willing to speculate about "dozens or more parasites joining the fray …." The court concluded that "while the trespass theory has some merit, there is insufficient proof of its elements to justify a preliminary injunction."

The *eBay/Register.com/Oyster* understanding of trespass to chattels grants website operators virtually unlimited control over the information that appears on their websites. Indeed, this control vastly exceeds what the "sweat of the brow" doctrine granted publishers. Under "sweat of the brow," the publisher had to expend resources in gathering information, and the defendant had to engage in wholesale copying of the compilation. Under the *eBay/Register.com/Oyster* approach, retrieving even one piece of information from a website could be unlawful because it involves use of the website operator's computer.

Computer Fraud and Abuse Act

The CFAA is the primary vehicle the federal government uses to prosecute computer crime. In 1996, Congress amended the CFAA to impose liability on whomever "intentionally accesses a computer without authorization or exceeds authorized access,

and thereby obtains … information from any protected computer involved in interstate commerce." 18 U.S.C. § 1030(a)(2)(C). A "protected computer" is defined as a computer "which is used in interstate or foreign commerce or communication…." § 1030 (e)(2)(B). Thus, any computer that is connected to the Internet is a "protected computer." (The CFAA contains other offenses, but this article will focus on this offense because it is the broadest.)

Although primarily a criminal statute, the CFAA permits a private cause of action to be brought by "[a]ny person who suffers damage or loss by reason of a violation of this section…." § 1030(g). When Congress first created the private cause of action, it contained ambiguous terms that confused courts and litigants and thus reduced its effectiveness. The USA-PATRIOT Act passed by Congress in the wake of the September 11, 2001, attacks amended the CFAA to eliminate these ambiguities. The term "loss" is defined 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." § 1030(e)(11).

The statute also contains clear jurisdictional thresholds for the bringing of a private action. The threshold of greatest relevance in database cases is that the conduct at issue caused "loss to 1 or more persons during any 1-year period … aggregating at least $5,000 in value." § 1030(a)(5)(B)(i).

Putting this all together, a person incurs civil liability under the CFAA if he obtains information without authorization from a website, and thereby causes loss of $5,000. "Loss" includes the cost of responding to the offense or conducting a damage

assessment. Thus, a website operator can obtain injunctive relief and an award of economic damages against a person who extracts without authorization one fact from its website, provided that the operator spends $5,000 on a "damage assessment."

Prior to the amendment of the CFAA in the USA PATRIOT Act, two courts found CFAA violations based upon the extraction of information from online databases. In both cases, the courts experienced difficulty interpreting and applying the $5,000 threshold, but nonetheless found liability. The recent amendments to the CFAA provide courts with a much clearer roadmap concerning the threshold.

The court in *Register.com v. Verio,* cited above, ruled that Register.com was likely to prevail on its CFAA claims arising from Verio's use of an Internet search robot to extract raw facts from Register.com's publicly accessible WHOIS database. The court concluded that Verio exceeded authorized access on the grounds that Verio did not comply with Register.com's demands that it cease extracting information, and that Verio's extraction of information for marketing purposes violated the terms of service posted on the Register.com website. The court rejected Verio's defense that Register.com's agreements with the Internet Corporation for Assigned Names and Numbers obligated it to make the information available.

The court had somewhat more difficulty meeting the $5,000 threshold. It speculated that if it did not enjoin Verio, then other vendors would use search robots; that these search robots would cause Register.com's computer to malfunction or crash; and that the malfunction or crash would cause at least $5,000 of economic damage.

One year later, the U.S. Court of Appeals for the First Circuit in *EF Cultural Travel v. Explorica*, 274 F.3d 577 (1st Cir. 2001) had an easier time meeting the $5,000

threshold because the plaintiff actually incurred $5,000 of costs. EF was an established tour company that offered student travel services. Several ex-employees of EF organized Explorica to compete with the EF in the student travel market. In order to determine the prices EF was charging for its tours so that it could underprice them, Explorica used an Internet "scraper" program designed specifically to mine all the necessary price information from the EF website. The scraper ultimately sent 60,000 inquiries to EF's website.

The court found that in developing the scraper program, Explorica used proprietary EF travel codes that Explorica employees had obtained under a confidentiality agreement when they worked for EF. For the First Circuit, this breach of the confidentiality agreement constituted the exceeding of authorized access. The court concluded that "Explorica's wholesale use of EF's travel codes to facilitate gathering EF's prices from its website reeks of use – and, indeed abuse – or proprietary information that goes beyond any authorized use of EF's website."

The First Circuit further concluded that the $20,044 EF spent to assess whether its website had been compromised satisfied the $5,000 loss threshold. The recent amendments to the CFAA are consistent with this holding; the definition of "loss" now explicitly includes "the cost of responding to an offense [and] conducting a damage assessment…." § 1030(e)(11).

The presence of a confidentiality agreement with a former employee appears at first blush to distinguish *Explorica* from the typical case of a bot searching a publicly accessible website for information. By focusing on the breach of the confidentiality agreement, the *Explorica* court side-stepped the question of whether a robotic search of a

publicly accessible website could be in excess of authorized access. However, the *Register.com* court suggested that a terms of service agreement prohibiting the use of bots would be sufficient to render any robotic search either unauthorized or in excess of authorized access. And if the website operator expended $5,000 on a damage assessment after a robotic search in violation of the terms of service, the *prima facie* elements of a CFAA violation would seem to be met.

Limiting Principles

This survey of trespass to chattels and CFAA cases suggests that online database publishers in the U.S. have two new powerful tools to prevent unauthorized copying of the information in their databases. Under *Oyster*, any unauthorized use of the server storing the information triggers trespass liability. And under the CFAA as amended, a publisher can prevent the unauthorized extraction of information so long as it is willing to expend $5,000 on a damage assessment. As a practical matter, these two legal theories appear to confer *de facto* ownership over the facts contained in their databases. However, some limiting principles may exist.

1. Trespass to Chattels. Several law review articles have suggested that the easy-to-satisfy *eBay/Register.com/Oyster* standard for trespass to chattels deviates from the historical roots of this common law doctrine by abandoning the requirement of real interference with the enjoyment of the chattel. Perhaps appellate courts will start to steer the trespass to chattels doctrine back to more traditional standards. But if they do not, a Constitutional argument can be leveled against application of the trespass to chattels doctrine to online databases.

The constitutional analysis begins with the Supreme Court's decision in *Feist v. Rural Telephone*. There, the unanimous Court held that "no one may copyright facts or ideas." Significantly, the *Feist* Court based its ruling not on the Copyright Act, but on the Intellectual Property Clause of the U.S. Constitution. Article I, Section 8, cl. 8 authorizes Congress "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors … the exclusive Right to their Respective Writings…" From this clause, the Court inferred that "[o]riginality is a constitutional requirement" for copyright protection, and held that facts by definition are not original. They are discovered rather than created.

Can database publishers employ a state common law doctrine to prohibit activity clearly permitted by the Intellectual Property Clause as interpreted by the Supreme Court in *Feist*? The constitutional preemption doctrine, flowing from the U.S. Constitution's Supremacy Clause, suggests not. Constitutional preemption precludes the states from "interfer[ing] with the federal policy … of allowing free access to copy whatever the federal patent and copyright laws leave in the public domain." *Bonito Boat v. Thunder Craft Boats*, 489 U.S. 141 (1989). The Court explained there that "[t]he offer of federal protection from competitive exploitation of intellectual property would be rendered meaningless in a world where substantially similar state law protections were readily available."

As the Supreme Court made clear in *Feist*, the Constitution's Intellectual Property Clause precludes copyright protection for facts: "the raw facts may be copied at will." A trespass to chattels claim, where the only "harm" to the computer is its use for the purpose of extracting facts, clearly interferes with this Constitutional imperative.

2. CFAA. The few CFAA cases to date suggest that the *Register.com* court may have erroneously interpreted the phrase "access a computer without authorization or exceeds authorized access" to include use of a publicly available website in a manner prohibited by the terms of service agreement. In *America Online v. LCGM*, 46 F.Supp.2d 444 (E.D. Va. 1998), for example, the defendant harvested email addresses from chatroom participants by "using [] software to evade AOL's filtering mechanisms." In these cases, as in *Explorica*, the unauthorized access involved far more than disregarding a statement posted on a publicly available website. Arguably, a defendant exceeds authorized access under the CFAA in an online database case only when the defendant circumvents technological protection measures or uses trade secret information to expedite extraction of the data.

Additionally, the term "loss" is now defined as "any reasonable cost to any victim…." The word "reasonable" may act as a limiting factor. A court could determine that Congress did not want a website operator's over-reaction to a minor violation to enable the operator to overcome the $5,000 loss threshold. Arguably, the operator's response would have to be proportionate to the single act violating the statute.

If these arguments fail, constitutional attacks can be leveled against application of the CFAA in this manner. These arguments would differ from the discussion of constitutional preemption above because the CFAA is a federal act passed by Congress, rather than state common law. Instead of focusing on the conflict between federal and state law, the constitutional argument here would center on the conflict between Congress' power under the Intellectual Property Clause and its power under the Commerce Clause.

The Supreme Court in *Railway Labor Executives v. Gibbons*, 455 U.S. 457 (1982), considered a statute enacted by Congress pursuant to the Commerce Clause which provided protection to employees of a railroad in bankruptcy. The Court held that the statute was inconsistent with the uniformity requirement of the Bankruptcy Clause. The Court further held that Congress cannot avoid the particular requirements of one enumerated power -- such as the uniformity requirement of the Bankruptcy Clause -- by relying on the generality of the Commerce Clause.

Congress enacted the CFAA pursuant to its power under the Commerce Clause. But under *Railway Labor*, Congress may not invoke the commerce power to do what the Intellectual Property Clause bars it from doing: granting exclusive rights in facts.

Of course, the reasoning of *Railway Labor* does not invalidate the CFAA *per se*; it just precludes its application to the extraction of facts from publicly accessible online databases. In a case involving real hacking or damage to a computer system, the CFAA would protect interests different from those addressed by the Intellectual Property Clause, *i.e.*, computer security. In database cases, however, the interests are identical -- the copying of facts.

In addition to conflicting with the Intellectual Property Clause, the CFAA as applied to database cases also raises serious First Amendment concerns. It is well settled that copyright's abhorrence of protection for facts has a clear First Amendment dimension. *Harper & Row v. Nation Enterprises*, 471 U.S. 539 (1985). This First Amendment opposition to a copyright monopoly over facts applies with equal force to a CFAA monopoly over facts.

Conclusion

In the future, many facts will be available to the public only via the Internet. If constitutionally imposed limits on the ownership of information are to continue to have any meaning in the digital age, courts must reject the application of trespass to chattels and the CFAA as alternate forms of database protection. Otherwise, courts in effect will permit a publisher to prohibit unilaterally the copying of facts from its publicly available website simply by posting a terms of service agreement forbidding such copying on its home page. This would contravene the United States' fundamental information policy articulated in *Feist*: "all facts -- scientific, historical, biographical, and news of the day …. are part of the public domain available to every person." In place of this policy, courts would impose a more restrictive policy similar to that underlying the EU Database Directive.