Cases illustrating the limitations of existing legal protections for online privacy
Cyberlaw (Law 276.1 and IS 235)
Fall 2002
Prof. Pamela Samuelson
Assignment originally scheduled for Sept. 30
(to be taught at first of two sessions on 10/2/02)

In re PHARMATRAK, INC. PRIVACY LITIGATION
United States District Court for Massachusetts
-- F. Supp.2d – (D. Mass. 2002)

Tauro, J.

Plaintiffs allege that Defendants "secretly intercepted and accessed Internet users' electronic communications with various health-related and medical-related Internet Web sites and secretly accessed their computer hard drives in order to collect private information about their Web browsing habits [and] confidential health information without their knowledge, authorization, or consent." Plaintiffs contend that the Pharmaceutical Defendants conspired with Plaintiff Pharmatrak to "collect and share this wrongfully obtained personal and sensitive information." This activity was allegedly accomplished through the use of "web bugs," "persistent cookies," and other devices. See Reno v. ACLU, 512 U.S. 844 (1997) (discussing the Internet); In re DoubleClick Inc. Privacy Litigation, 154 F.Supp.2d 497, 500-505 (S.D.N.Y. 2001) (discussing the Internet, the Web, cookies, and data collection).
…

The Pharmaceutical Defendants hired Defendant Pharmatrak to monitor their corporate web sites and provide monthly analysis of web site traffic. Pharmatrak offered its clients two relevant products: NETcompare, which was designed to monitor activity across clients' web pages, and DRUGcompare, which was designed to monitor activity across disease categories and drug product pages. All of the Pharmaceutical Defendants purchased NETcompare, and Defendant Pharmacia may have licensed DRUGcompare during testing phases. Pharmatrak specifically represented to the Pharmaceutical Defendants that these products did not collect "personally identifiable information." Even though the Pharmaceutical Defendants may not have known precisely how Pharmatrak's software worked, Plaintiffs readily admit that "the Pharmaceutical Defendants did authorize Pharmatrak's presence upon their Web sites . . . ." Pharmatrak's system operated through the use of HTML programming, JavaScript programming, cookies, and "web bugs." Each of the Pharmaceutical Defendants' web pages were programmed with Pharmatrak code, which allowed Pharmatrak to monitor web site activity. When a computer browser requested information from a Pharmaceutical Defendant's web page, the web page would send the requested information to the user, and the site's programming code would instruct the user's browser to contact Pharmatrak's web server and retrieve a "clear GIF" from it. A clear GIF is a one pixel-by-one pixel or two pixels-by-two pixels graphic image, and is sometimes called a web bug or a "pixel tag." The purpose of a clear GIF was to cause the

user's computer browser to communicate directly with Pharmatrak's web server. Some communications may have also included code referencing JavaApplet, a software program that runs in a user's browser, or JavaScript, an Internet programming language.

Having caused the user's Internet browser to contact Pharmatrak, Pharmatrak then sent a cookie back to the browser. A cookie is an electronic file "attached" to a user's computer by a computer server. Plaintiffs concede that "[c]ookies generally perform many convenient and innocuous functions." Commonly, cookies are used to store users' preferences and other information, which allows users to easily access and utilize personalized services on the web or to maintain an online "shopping cart." Cookies also allow web sites to differentiate between users as they visit by assigning each individual browser a unique, randomly generated numeric or alphanumeric identifier. If an individual browser had already visited the "Pharmatrak-enabled" website, Pharmatrak would recognize the previously placed cookie and could therefore differentiate between a repeat visit and an initial visit. Pharmatrak programmed its cookies to expire after 90 days.

It is possible that many individual users were unaware that, in addition to their browser communicating with a Pharmaceutical Defendant's web site, it was also communicating with Pharmatrak. Plaintiffs allege that the JavaApplet used by Pharmatrak allowed Pharmatrak to monitor the length of time that a particular user viewed one of the Pharmaceutical Defendants' web pages. Plaintiffs also allege that the JavaScript programming allowed Pharmatrak to "intercept the full URL of the tracked Web page visited by the user," as well as "the full URL of the Web page visited by the Internet user *immediately prior* to the user's visit to the Pharmatrak-coded Web page. This prior Web page address is know as a 'referrer URL.'" According to Plaintiffs, Pharmatrak used JavaScript "to extract referring URLs from the client's history, thereby bypassing any security or privacy mechanisms put in place to control the flow of potentially sensitive data." The JavaScript and JavaApplet, therefore, also caused users' computer browsers to communicate with Pharmatrak's server while they intentionally communicated with the Pharmaceutical Defendants' servers.

Plaintiffs also assert that Pharmatrak was able to "Capture [] Personal Information Submitted by Internet Users to the Pharmaceutical Defendants' Web Sites." Users submitted this information in two ways. First, an individual could use the "POST" method, and voluntarily fill out an online form in order to register with the site, or to receive mailings, a rebate, or other information. For example, an individual wishing to view the full text of articles on nytimes.com must first register with the site, a process which requires the individual to volunteer certain information. Second, an individual using the "GET" method could perform an online search, resulting in a URL with search terms appended to it. The appended information is known as the "query string." For example, a person interested in Cornell Law School could perform a search resulting in the following URL: http://search.yahoo.com/bin/search?p=cornell+law+school. All of the material following the question mark (i.e. p=cornell+law+school) is known as the query string, and is "rich in useful content." Plaintiffs allege that Pharmatrak was able to

intercept and collect detailed, specific information about individual users from the full URLs, and place the information into relational databases.

Plaintiffs' computer scientist, C. Matthew Curtin, and his company, Interhack, examined Pharmatrak's servers between December 17, 2001 and January 18, 2002, pursuant to the court's Order. The examination of Pharmatrak's logs "identified hundreds of people by name." Based on Curtin's analysis, Plaintiffs claim that Pharmatrak collected information which included: names, addresses, telephone numbers, dates of birth, sex, insurance status, medical conditions, education levels, and occupations. Pharmatrak also collected data about email communications, including user names, email addresses, and subject lines from emails. Although Plaintiffs submit no evidence that Pharmatrak collected, sorted, or assembled this information into detailed "profiles," other than the aggregate information it submitted to the Pharmaceutical Defendants, Curtin did build such profiles. Curtin also asserts that it would be possible to build detailed profiles of individuals using the data collected by Pharmatrak and matching it to "another data source, such as a telephone book." Again, however, there is no evidence that Pharmatrak ever attempted to do so.

In sum, Plaintiffs argue that "Pharmatrak's technology permits defendants to collect extensive, detailed information about plaintiffs and Class members." In addition to the personal information discussed above, the information collected allegedly included "Web sites the Internet users were at prior to the time they went to the Pharmaceutical Defendants' Web sites, questions they asked and typed in at those prior sites, information they entered while at the Pharmaceutical Defendants' web sites, and the types of computers they were using."

…

Plaintiffs seek summary judgment against Defendants Pharmatrak and Glocal, and Defendants each seek summary judgment against Plaintiffs.

A. Count I - The Wiretap Act

Title I of the Electronic Communication Privacy Act of 1986 ("ECPA"), Interception of Electronic Communications ("The Wiretap Act"), provides that:

> Except as otherwise specifically provided in this chapter[,] any person who – (a) intentionally intercepts, endeavors to intercept, or procures any other person 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).

This criminal statute provides for a private right of action, and is subject the following statutory
exception:

> (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 . . . .

…

Plaintiffs claim that "Pharmatrak intercepted plaintiffs' transmission of their personal information to the Pharmaceutical Defendants' Web sites without the express or implied consent of either plaintiffs or the Pharmaceutical Defendants." Despite the fact that the Pharmaceutical Defendants may have consented to Pharmatrak's assembly of anonymous, aggregate information, Plaintiffs insist that the web sites never consented to Pharmatrak's collection of personally identifiable information. Absent this specific consent, Plaintiffs argue, the Wiretap Act's statutory exception simply does not apply.

Pharmatrak concedes that the Pharmaceutical Defendants did not consent to the collection of personally identifiable information. According to Pharmatrak, however, the relevant inquiry is whether the Pharmaceutical Defendants consented to Pharmatrak's NETcompare *service*, i.e. the collection of data from the Pharmaceutical Defendants' web sites, regardless of how the service eventually operated. It is undisputed that the Pharmaceutical Defendants contracted with Defendant Pharmatrak to obtain data regarding their web sites, and that they proceeded to have the Pharmatrak code placed on the web sites. Pharmatrak, therefore, asserts that the statutory exception for consent has been met, and that it is entitled to summary judgment on the Wiretap Act claim.

In In re DoubleClick Inc. Privacy Litigation ("DoubleClick"), the Southern District of New York disposed of a multidistrict consolidated class action case pursuant to Rule 12(b)(6). There, the plaintiffs alleged that DoubleClick, an Internet advertising firm, placed cookies on their computers, thereby collecting "information that Web users, including plaintiffs and the Class, consider to be personal and private, such as 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."

The DoubleClick court found that the web sites affiliated with DoubleClick were "'parties to the communication[s]' from plaintiffs and have given sufficient consent to DoubleClick to intercept them," despite the possibility that the plaintiffs may not have known that their computers were communicating with DoubleClick, and that the affiliated Web sites may not have fully understood the mechanisms of the DoubleClick service.

Having found consent, the DoubleClick court proceeded to analyze Section 2511(2)(d)'s "criminal" or "tortious" purpose requirement, which "is to be construed narrowly." The court noted that the evidence in the case suggested that DoubleClick's actions were motivated by legitimate business goals, and found an "utter lack of evidence that [DoubleClick's] intent was tortious . . . ." Because it found that DoubleClick acted with consent and without a tortious or criminal purpose, the court dismissed the plaintiffs' Wiretap Act claim.

In Chance v. Avenue A. Inc., 165 F.Supp.2d 1153 (W.D. Wash. 2001), the plaintiffs alleged that Avenue A had placed cookies on their computers, thus permitting the company to surreptitiously monitor plaintiffs' electronic communications. First, addressing consent, the court held that "[i]t is implicit in the web pages' code instructing the user's computer to contact Avenue A, either directly or via DoubleClick's server, that the web pages have consented to Avenue A's interception of the communication between them and the individual user." The court also found that the plaintiffs had presented no evidence that the defendants acted with a tortious or illegal purpose and, therefore, granted summary judgment on the claim to Avenue A.

In the present case, Plaintiffs concede that the Pharmaceutical Defendants consented to the placement of code for Pharmatrak's NETcompare service on their web sites. As was the case in DoubleClick and Avenue A, the web site Defendants (here, the Pharmaceutical Defendants) consented to the service of a web-monitoring company (Pharmatrak), and such consent precludes a claim under the Wiretap Act. The Pharmaceutical companies contracted with Pharmatrak, and authorized Pharmatrak to communicate with any users who contacted the Pharmaceutical Web sites. Despite Plaintiffs' valiant attempts to shift the inquiry, it is irrelevant for the purposes of the Wiretap Act whether the Pharmaceutical Defendants knew the precise mechanisms of Pharmatrak's service or not. It is sufficient that the Pharmaceutical Defendants were parties to communications with Plaintiffs and consented to the monitoring service provided by Defendant Pharmatrak.

Plaintiffs are also unable to demonstrate that Defendants acted with a tortious purpose. Plaintiffs have produced no evidence "'either (1) that the primary motivation, or (2) that a determinative factor in the actor [Pharmatrak's] motivation for intercepting the conversation was to commit a criminal [or] tortious . . . act.'" Without a showing of the requisite *mens rea*, Plaintiffs cannot succeed on their claim under the Wiretap Act.

Because the Pharmaceutical Defendants consented to Pharmatrak's NETcompare service, and because Plaintiffs are unable to present any evidence whatsoever of a tortious intent, Defendants are entitled to summary judgment on Count I of the Complaint.

B. Count II - Stored Communications Act

Title II of the ECPA, also known as the "Stored Wire and Electronic Communications and
Transactional Records Act," "aims to prevent hackers from obtaining, altering, or destroying certain stored electronic communications." The statute provides:

> [W]hoever – (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 by subsection (b) of this section.

Plaintiffs acknowledge that § 2701 was primarily designed to provide a cause of action against computer hackers, and argue that "Defendants' conduct of accessing data in plaintiffs' computers, including the content of plaintiffs' e-mails, constitutes electronic trespassing and falls squarely within the ambit of Section 2701."

Defendants disagree, and claim that they are entitled to summary judgment on at least two separate grounds: (1) Plaintiffs' computers are not facilities which provide electronic communications services, an essential element of § 2701; and (2) any alleged access to "communications" was authorized.

Defendants are correct that an individual Plaintiff's personal computer is not a "facility through which an electronic communication service is provided" for the purposes of § 2701. Plaintiffs find it noteworthy that "[p]ersonal computers provide consumers with the opportunity to access the Internet and send or receive electronic communications," and that "[w]ithout personal computers, most consumers would not be able to access the Internet or electronic communications." Fair enough, but without a telephone, most consumers would not be able to access telephone lines, and without televisions, most consumers would not be able to access cable television. Just as telephones and televisions are necessary devices by which consumers access particular services, personal computers are necessary devices by which consumers connect to the Internet. While it is possible for modern computers to perform server-like functions, there is no evidence that any of the Plaintiffs used their computers in this way. While computers and telephones certainly provide services in the general sense of the word, that is not enough for the purposes of the ECPA. The relevant *service* is Internet access, and the service is provided through ISPs or other servers, not through Plaintiffs' PCs.

Even if the court were to assume that Plaintiffs' computers are "facilities" under § 2701, any access to stored communications was authorized and, thus, Defendants' conduct falls under the exception from liability created by § 2701(c)(2). As was the case in DoubleClick and Avenue A, the Pharmaceutical Defendants are "users" under the ECPA. The DoubleClick court noted that, "in a practical sense, Web sites are among the most active 'users' of Internet access." As users, the Pharmaceutical Defendants could consent to Pharmatrak's interception of Plaintiffs' communications, and Plaintiffs cannot survive the motions for summary judgment "based solely on the naked allegation that defendant[s'] access was 'unauthorized.'"

Plaintiffs argue that this case is factually different from DoubleClick, because the Pharmaceutical Defendants did not know that Pharmatrak would collect the type and amount of personally identifiable information that it did. Even viewing this factual distinction in the light most favorable to Plaintiffs, the Pharmaceutical Defendants nonetheless authorized Pharmatrak to monitor electronic communications between the web sites and Plaintiffs. As discussed above [], the PharmaceuticalDefendants consented

to the monitoring service provided by Defendant Pharmatrak in NETcompare, even if they were unaware that the program was able to identify personal information.

In addition, the ECPA does not prohibit Pharmatrak's actions with regard to the placing of cookies on Plaintiffs' computers. Section § 2701 seeks to target communications which are in "electronic storage" incident to their transmission. This court agrees with the DoubleClick court that "Title II 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 store it." Even if such cookies were covered by the ECPA, Pharmatrak created and sent the cookies, and thus any accessing of the cookies by Pharmatrak at a later date would certainly be "authorized." Because Pharmatrak's cookies fall outside the scope of § 2701, Plaintiffs' claim under that section must fail.

Finally, Plaintiffs persistently argue that the Pharmaceutical Defendants did not consent to the allegedly improper interception of personal information. If the Pharmaceutical Defendants did not consent to the alleged interception of personally identifiable information, then they could not have "intentionally access[ed] without authorization" any electronic communications. Without the necessary intent under this punitive statute, the Pharmaceutical Defendants cannot be held liable and are entitled to summary judgment.

Accordingly, all Defendants are entitled to summary judgment on Count II.

C. Count III - Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) creates a claim against:

> (a) Whoever – . . . (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . (c) information from any protected computer if the conduct involved an interstate or foreign communication . . .

The CFAA limits recovery to those persons who suffer "damage or loss by reason of a violation" of the Act. Section 1030(e)(8) defines damage as "any impairment to the integrity or availability of data, a program, a system, or information, that – (A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals. . . ." Plaintiffs do not allege that their computers were physically damaged in any way, or that they suffered any damage resulting from the repair or replacement of their computer systems. Instead, Plaintiffs argue that their "sensible interpretation" of the CFAA allows recovery for a "cognizable 'loss,'" as distinct from economic damage, for the invasion of their privacy and the "concomitant loss of control over the dissemination of their private information." Plaintiffs stress that they allege both loss and damages, and that the damage threshold of $5,000 may be met by aggregating claims among individuals and over a one year period. The CFAA does not define "loss," and the First Circuit noted in EF Cultural Travel BV, et. al. v. Explorica that "[f]ew courts have

endeavored to resolve the contours of damage and loss under the CFAA." In that case, the First Circuit explicitly agreed with the DoubleClick court, and concluded that the statute's use of "damage or loss" indicated a Congressional desire to allow recovery for more than purely physical damage. The First Circuit was careful to note, however, that it did not hold that any loss is compensable, and that "Congress could not have intended other types of loss to support recovery unless [the $5,000] threshold were met." Plaintiffs have not shown any evidence whatsoever that Defendants have caused them at least $5,000 of damage or loss. Even accepting Mr. Curtin's bald assertion that "[d]ata about people are valuable, marketable assets," Plaintiffs are unable to meet the statutory threshold. Any damage or loss under the CFAA may be aggregated across victims and across time, but only for a single act. Because Plaintiffs have not shown any facts that demonstrate damage or loss of over $5,000 for any single act of the Defendants, Defendants are entitled to summary judgment on Count III.

Comments and Questions

1. As the Pharmatrak case illustrates, persons who surf the Web may be ignorant of being monitored. Senators Edwards and Hollings introduced S. 197, the Spyware Control and Privacy Protection Act of 2001, in the 107th Congress to require firms to give notice if their software contains surveillance capabilities. The bill would also require disclosure of what information being collected and to whom it will be sent. Firms would also have to provide information about how to disable spyware features. It would also require that users provide affirmative consent before spyware capabilities could be enabled. Violations of the law would give a private right of action to injured persons, allowing recovery of actual monetary losses or $2500 for each violation not to exceed $500,000. What are the pros and cons of such a bill? Would legislation of this sort have provided adequate relief to the plaintiffs here?

2. The European Union (EU) has adopted comprehensive privacy regulations to protect its citizens against unauthorized collection, processing and reuse of personal data by third parties. See Directive 95/46/EC of the European Parliament and the Council, October 25, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Community, L281 (Nov. 23, 1995). Article 6 of this Directive requires member states of the EU to provide, among other things, that personal data must be "(b) collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes." Article 7 goes on to provide that EU member states shall allow personal data to be processed only if: (a) the data subject has unambiguously given his consent; (b) the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation, (d) the processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in…a third party to whom the data are disclosed. The Directive was meant to regulate data collection and processing by non-governmental actors (that is, by businesses and other organizations). Article 25 of the EU

data protection directive provides that member states of the EU "shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if…the third country in question ensures an adequate level of protection" for personal data. More recently, the EU has issued Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal of the European Community L 201/37 (July 31, 2002) to supplement other EU information privacy directives and update EU privacy principles to apply to advanced digital technologies and the Internet. US and EU officials negotiated "safe harbor" rules allowing U.S. firms to collect and process data on Europeans as long as they comply with specified fair information privacy principles. See U.S. Department of Commerce, Safe Harbor Privacy Principles (July 21, 2000). What are the implications of the EU directive for pharmaceutical companies or for Pharmatrak as to EU citizens who might have visited websites surveilled by Pharmatrak's software?

3. During the 1990's, partly as a result of pressure from the EU and partly in order to stimulate the growth of e-commerce, U.S. government officials strongly urged firms to adopt "fair information practices" to protect online privacy and to post and abide by privacy policies on their websites. The Federal Trade Commission articulated five core privacy principles in Privacy Online: A Report to Congress (June 1998): (1) users should have notice of a firm's information practices before any personal information is collected from them, including what information is collected, by whom, and for what purposes, (2) users should have a choice about whether data can be collected about them and about whether such data can be disclosed to others or reused for other purposes, (3) users should be able to access to information collected about them and to contest the accuracy of the information, (4) firms should take other reasonable measures to ensure that data collected is accurate and secure against unauthorized disclosures and access (e.g., by use of encryption to protect the information in transit or in a stored area), and (5) a simple means should exist to enforce fair information practices and obtain redress for grievances. Would adoption of these fair information practices have averted the online privacy complaint in the *Pharmatrak* case?

4. Under its authority to challenge unfair or deceptive practices in section 5 of the Federal Trade Commission Act, the Federal Trade Commission has initiated proceedings against firms for violating posted online privacy policies. For example, the FTC initiated charges against Toysmart.com after the firm went into bankruptcy because the bankruptcy trustee planned sell the firm's customer lists (one of its few assets) in violation of its online privacy policy which had promised consumers that any personal information collected by the firm would not be shared with third parties. See FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations, available at http://www.ftc.gov/2000/07/toysmart2.htm.

5. The law review literature about online privacy is vast. Among the better works are: Paul M. Schwartz, Privacy and Democracy in Cyberspace, 52 Vand. L. Rev. 1609 (1999) and Daniel J. Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087 (2002). An especially good resource is Volume 52, issue 1 of the Stanford Law Review (May 2000)

that features several articles and essays about cyberspace privacy issues by, among others, Anita L. Allen, Julie E. Cohen, Richard A. Epstein, A. Michael Froomkin, David G. Post, Jessica Litman, Pamela Samuelson, Eugene Volokh, Jonathan Weinberg, and Jonathan Zittrain. See also Whitfield Diffie and Susan Landau, Privacy on the Line: The Politics of Wiretapping and Encryption, Cambridge MA: MIT Press, 1998; Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century, Sebastopol CA: O'Reilly & Associates, 2000; Peter P. Swire and Robert E. Litan, None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive, Washington DC: Brookings Institution Press, 1998.

6. The Electronic Privacy Information Center provides a useful website for tracking privacy-related legislation pending before Congress. See http://www.epic.org/privacy/bill_track.html.

7. There are many reasons why the U.S. has not adopted comprehensive information privacy laws akin to those in the EU. For one thing, Americans are generally more trusting of the private sector and of the market than the Europeans. They think it is better for firms to adopt standards voluntarily and to abide by them rather than to have the government adopt strict rules which the industry may ignore or subvert. Second, Americans tend to believe in the power of the mass media to hold private sector abuses in check. Third, Americans are inclined to think that technologies, such as the World Wide Web Consortium's Platform for Privacy Preferences, can contribute to solutions of problems created by technologies. In addition, even when Americans are considering government intervention, they are much more inclined than Europeans to engage in a cost-benefit analysis about regulatory alternatives. Identifying a market failure may suggest the need for government intervention, but Americans are more likely to go on to inquire whether possible unintended consequences of a proposed regulation will make the cure worse than the disease. Moreover, Americans are more inclined to adopt reactive rather than proactive regulations. That is, they are generally disinclined to regulate until problems have actually occurred, and they prefer to tailor regulatory solutions to those problems rather than to adopt broad regulations anticipating problems yet to arise. Finally, Americans are more prone to adopt regulations that give consumers information about private sector practices so consumers can exercise their market power to shop for firms with good privacy policies. Once they have such information, Americans tend to think that the market will work things out. Consumers who are averse to reuses of their personal data will, in this view, shift their business to firms that respect their privacy preferences. Yet it must be said that the Direct Marketing Association is also a powerful lobbying organization, as are many of the organizations (such as the pharmaceutical companies) who use direct marketing techniques to reach their customers.

8. Efforts to use common law torts to protect electronic privacy have generally been unsuccessful. See also Dwyer v. American Express, 273 Ill. App. 3d 742, 652 N.E.2d 1351 (Ill. App. 1st Dist. 1995). Dwyer complained that American Express had breached his common privacy rights by compiling lists of his and other customers' buying habits and renting them to

third parties. The court dismissed the complaint, saying that "[b]y 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." Are there any limits to what American Express might do with customer data?

Smyth v. Pillsbury Co.
United States District Court for the Eastern District of Pennsylvania
914 F. Supp. 97 (E.D. Pa. 1996)

Weiner, J.

In this diversity action, plaintiff, an at-will employee, claims he was wrongfully discharged from his position as a regional operations manager by the defendant. Presently before the court is the motion of the defendant to dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. For the reasons which follow, the motion is granted….

Defendant maintained an electronic mail communication system ("e-mail") in order to promote internal corporate communications between its employees. Defendant repeatedly assured its employees, including plaintiff, that all e-mail communications would remain confidential and privileged. Defendant further assured its employees, including plaintiff, that e-mail communications could not be intercepted and used by defendant against its employees as grounds for termination or reprimand.

In October 1994, plaintiff received certain e-mail communications from his supervisor over defendant's email system on his computer at home. In reliance on defendant's assurances regarding defendant's e-mail system, plaintiff responded and exchanged e-mails with his supervisor. At some later date, contrary to the assurances of confidentiality made by defendant, defendant, acting through its agents, servants and employees, intercepted plaintiffs private email messages made in October 1994. On January 17, 1995, defendant notified plaintiff that it was terminating his employment effective February 1, 1995, for transmitting what it deemed to be inappropriate and unprofessional comments[1] over defendant's e-mail system in October, 1994.

As a general rule, Pennsylvania law does not provide a common law cause of action for the wrongful discharge of an at-will employee such as plaintiff. Pennsylvania is an employment at-will jurisdiction and an employer "may discharge an employee with or without cause, at pleasure, unless restrained by some contract." Henry v. Pittsburgh & Lake Erie Railroad Co., 139 Pa. 289, 297, 21 A. 157, 157 (1891). See also, Brown v. Hammond, 810 F. Supp. 644, 645 (E.D. Pa. 1993) (An employer's right to terminate an at-will employee is "virtually absolute")….

Plaintiff claims that his termination was in violation of "public policy which precludes an employer from terminating an employee in violation of the employee's right

---

[1] Defendant alleges in its motion to dismiss that the e-mails concerned sales management and contained threats to "kill the backstabbing bastards" and referred to the planned Holiday party as the " Jim Jones Koolaid affair."

to privacy as embodied in Pennsylvania common law." Complaint at P 15.[2] In support for this proposition, plaintiff directs our attention to a decision by our Court of Appeals in Borse v. Piece Goods Shop, Inc., 963 F.2d 611 (3d Cir. 1992). In Borse, the plaintiff sued her employer alleging wrongful discharge as a result of her refusal to submit to urinalysis screening and personal property searches at her work place pursuant to the employer's drug and alcohol policy. After rejecting plaintiff's argument that the employer's drug and alcohol program violated public policy encompassed in the United States and Pennsylvania Constitutions, our Court of Appeals stated "our review of Pennsylvania law reveals other evidence of a public policy that may, under certain circumstances, give rise to a wrongful discharge action related to urinalysis or to personal property searches. Specifically, we refer to the Pennsylvania common law regarding tortious invasion of privacy." Id. at 620.

The Court of Appeals in Borse, observed that one of the torts which Pennsylvania recognizes as encompassing an action for invasion of privacy is the tort of "intrusion upon seclusion." As noted by the Court of Appeals, the Restatement (Second) of Torts defines the tort as follows:

> 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 § 652B. Liability only attaches when the "intrusion is substantial and would be highly offensive to the 'ordinary reasonable person.'" Borse, 963 F.2d at 621 (citation omitted). Although the Court of Appeals in Borse observed that "the Pennsylvania courts have not had occasion to consider whether a discharge related to an employer's tortious invasion of an employee's privacy violates public policy", the Court of Appeals predicted that in any claim where the employee claimed that his discharge related to an invasion of his privacy "the Pennsylvania Supreme Court would examine the facts and circumstances surrounding the alleged invasion of privacy. If the court determined that the discharge was related to a substantial and highly offensive invasion of the employee's privacy, [the Court of Appeals] believe that it would conclude that the discharge violated public policy." Id. at 622. In determining whether an alleged invasion of privacy is substantial and highly offensive to a reasonable person, the Court of Appeals predicted that Pennsylvania would adopt a balancing test which balances the employee's privacy interest against the employer's interest in maintaining a drug-free workplace. Id. at 625. Because the Court of Appeals in Borse could "envision at least two ways in which an employer's drug and alcohol program might violate the public

---

[2] Although plaintiff does not affirmatively allege so in his Complaint or in his memorandum of law in opposition to defendant's motion to dismiss, the allegations in the Complaint might suggest that plaintiff is alleging an exception to the at-will employment rule based on estoppel, i.e. that defendant repeatedly assured plaintiff and others that it would not intercept e-mail communications and reprimand or terminate based on the contents thereof and plaintiff relied on these assurances to his detriment when he made the "inappropriate and unprofessional" e-mail communications in October 1994. The law of Pennsylvania is clear, however, that an employer may not be estopped from firing an employee based upon a promise, even when reliance is demonstrated. Paul v. Lankenau Hospital, 524 Pa. 90, 569 A.2d 346 (1990).

policy protecting individuals from tortious invasion of privacy by private actors" id. at 626, the Court vacated the district court's order dismissing the plaintiff's complaint and remanded the case to the district court with directions to grant Borse leave to amend the Compliant to allege how the defendant's drug and alcohol program violates her right to privacy.

Applying the Restatement definition of the tort of intrusion upon seclusion to the facts and circumstances of the case sub judice, we find that plaintiff has failed to state a claim upon which relief can be granted. In the first instance, unlike urinalysis and personal property searches, we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. Significantly, the defendant did not require plaintiff, as in the case of an urinalysis or personal property search to disclose any personal information about himself. Rather, plaintiff voluntarily communicated the alleged unprofessional comments over the company e-mail system. We find no privacy interests in such communications.

In the second instance, even if we found that an employee had a reasonable expectation of privacy in the contents of his e-mail communications over the company e-mail system, we do not find that a reasonable person would consider the defendant's interception of these communications to be a substantial and highly offensive invasion of his privacy. Again, we note that by intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects. Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.

Comments and Questions

1. In Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996) two police officers sued the City of Reno claiming violations of their privacy rights in online communications to stop an internal affairs investigation from getting access to, using, or disclosing messages they had sent to one another via the police department's network. The court concluded that Bohach and Catalano may have had a subjective expectation of privacy when using the network to communicate with one another (or else they would not have sent the indiscreet messages they did). However, they did not have an objectively reasonable expectation of privacy in the messages given the technical capabilities of the software (which regularly recorded traffic), policies of the department (which forbade use of the network to send certain kinds of messages, such as those in violation of anti-discrimination laws), and an announcement sent when the system was first installed informing users that messages would be "logged on the network."

2. Many employers regularly monitor Internet usage and email communications by employees which obviously reduces employee

expectations of privacy. See United States v. Simons, 206 F.2d 392 (4th Cir. 2000).

3. Should firms at least be required to announce that they are engaged in monitoring of Internet-based communications before doing it? Why have legislative efforts to require announcement of such monitoring met with resistance in state legislatures?

Konop v. Hawaiian Airlines, Inc.
United States Court of Appeals for the Ninth Circuit
2002 U.S. App. LEXIS 17586 (9th Cir. 2002)

Boochever, J.

FACTS

Konop, a pilot for Hawaiian, created and maintained a website where he posted bulletins critical of his employer, its officers, and the incumbent union, Air Line Pilots Association ("ALPA"). Many of those criticisms related to Konop's opposition to labor concessions which Hawaiian sought from ALPA. Because ALPA supported the concessions, Konop, via his website, encouraged Hawaiian employees to consider alternative union representation.

Konop controlled access to his website by requiring visitors to log in with a user name and password. He created a list of people, mostly pilots and other employees of Hawaiian, who were eligible to access the website. Pilots Gene Wong and James Gardner were included on this list. Konop programmed the website to allow access when a person entered the name of an eligible person, created a password, and clicked the "SUBMIT" button on the screen, indicating acceptance of the terms and conditions of use. These terms and conditions prohibited any member of Hawaiian's management from viewing the website and prohibited users from disclosing the website's contents to anyone else.

In December 1995, Hawaiian vice president James Davis asked Wong for permission to use Wong's name to access Konop's website. Wong agreed. Davis claimed he was concerned about untruthful allegations that he believed Konop was making on the website. Wong had not previously logged into the website to create an account. When Davis accessed the website using Wong's name, he presumably typed in Wong's name, created a password, and clicked the "SUBMIT" button indicating acceptance of the terms and conditions.

Later that day, Konop received a call from the union chairman of ALPA, Reno Morella. Morella told Konop that Hawaiian president Bruce Nobles had contacted him regarding the contents of Konop's website. Morella related that Nobles was upset by Konop's accusations that Nobles was suspected of fraud and by other disparaging statements published on the website. From this conversation with Morella, Konop believed Nobles had obtained the contents of his website and was threatening to sue Konop for defamation based on statements contained on the website.

After speaking with Morella, Konop took his website offline for the remainder of the day. He placed it back online the next morning, however, without knowing how Nobles

had obtained the information discussed in the phone call. Konop claims to have learned only later from the examination of system logs that Davis had accessed the website using Wong's name.

In the meantime, Davis continued to view the website using Wong's name. Later, Davis also logged in with the name of another pilot, Gardner, who had similarly consented to Davis' use of his name. Through April 1996, Konop claims that his records indicate that Davis logged in over twenty times as Wong, and that Gardner or Davis logged in at least fourteen more times as Gardner….

DISCUSSION

…

I. Electronic Communications Privacy Act Claims

We first turn to the difficult task of determining whether Hawaiian violated either the Wiretap Act, 18 U.S.C. § § 2510-2522 (2000) or the Stored Communications Act, 18 U.S.C. § § 2701-2711 (2000), when Davis accessed Konop's secure website. In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), which was intended to afford privacy protection to electronic communications. Title I of the ECPA amended the federal Wiretap Act, which previously addressed only wire and oral communications, to "address[]the interception of ... electronic communications." S. Rep. No. 99-541, at 3 (1986). Title II of the ECPA created the Stored Communications Act (SCA), which was designed to "address[]access to stored wire and electronic communications and transactional records." *Id.*

As we have previously observed, the intersection of these two statutes "is a complex, often convoluted, area of the law." *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998). In the present case, the difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results. *See. e.g.*, Tatsuya Akamine, Note, *Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer Is Subject to an Interception Under the Federal Wiretap Act*, 7 J.L. Pol'y 519, 521-29, 561-68 (1999) (criticizing the judiciary's interpretation of the ECPA). We observe that until Congress brings the laws in line with modern technology, protection of the Internet and websites such as Konop's will remain a confusing and uncertain area of the law.

A. The Internet and Secure Websites

The Internet is an international network of interconnected computers that allows millions of people to communicate and exchange information. The World Wide Web, the best known category of communication over the Internet, consists of a vast number of electronic documents stored in different computers all over the world. Any person or organization with a computer connected to the Internet can "publish" information on the Web in the form of a "web page" or "website." A website consists of electronic information stored by a hosting service computer or "server." The owner of the website may pay a fee for this service. Each website has a unique domain name or web address

(*e.g.*, Amazon. com or Lycos. com), which corresponds to a specific location within the server where the electronic information comprising the website is stored. A person who wishes to view the website types the domain name into a computer connected to the Internet. This is essentially a request to the server to make an electronic copy of the website (or at least the first page or "home page") and send it to the user's computer. After this electronic information reaches the user's computer, it is downloaded for viewing on the user's screen.

While most websites are public, many, such as Konop's, are restricted. For instance, some websites are password protected, require a social security number, or require the user to purchase access by entering a credit card number. The legislative history of the ECPA suggests that Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards. *See* S. Rep. No. 99-541, at 35-36 ("This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to ... electronic or wire communications that are not intended to be available to the public."); H.R. Rep. No. 99-647 at 41, 62-63 (1986) (describing the Committee's understanding that the configuration of the electronic communications system would determine whether or not an electronic communication was readily accessible to the public). The nature of the Internet, however, is such that if a user enters the appropriate information (password, social security number, etc.), it is nearly impossible to verify the true identity of that user.

We are confronted with such a situation here. Although Konop took certain steps to restrict the access of Davis and other managers to the website,[3] Davis was nevertheless

---

[3] Specifically, Konop configured the website to allow access when a person typed in the correct web address, received the home page of his website, entered the name of an eligible person, created a password, and clicked the "SUBMIT" button indicating acceptance of the terms and conditions of use. In addition, Konop displayed the following language on the home page of his website:

> This is the gateway for NEWS UPDATES and EDITORIAL COMMENTS directed only toward Hawaiian Air's pilots and other employees, not including HAL management. By entering, you acknowledge and agree to the terms and conditions of use as specified below. You must read this entire page before entry. Others should simply find *something else* to do with their time.
>
> If you are already a registered user, you may fill in your name along with the other information required below, then enter the system. If you want to visit the system, and you belong to the authorized group, you must supply the proper information before you will be allowed to enter. Make note of the password you enter for your first visit, otherwise future visits may be delayed. Visits by others will be strictly prohibited.

Beneath this language, Konop provided boxes for a person's name, occupation, email address and password. Below the boxes were two buttons: one said "SUBMIT," the other said "CLEAR." The advisement continued:

> All name and contact information will be kept strictly confidential. Any effort to defeat, compromise or violate the security of this website will be prosecuted to the fullest extent of the law.
> WARNING!
> The information contained herein is CONFIDENTIAL, and it is not intended for public dissemination! By requesting entry in the system, you must agree not to furnish any of the information contained herein to any other person or for any other use. Republication or redistribution of this information to any other person is strictly prohibited. Anyone found to

able to access the website by entering the correct information, which was freely provided to Davis by individuals who were eligible to view the website.

B. Wiretap Act

Konop argues that Davis' conduct constitutes an interception of an electronic communication in violation of the Wiretap Act. The Wiretap Act makes it an offense to "intentionally intercept[] ... any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). We must therefore determine whether Konop's website is an "electronic communication" and, if so, whether Davis "intercepted" that communication.

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, photoelectronic or photooptical system." *Id.* § 2510(12). As discussed above, website owners such as Konop transmit electronic documents to servers, where the documents are stored. If a user wishes to view the website, the user requests that the server transmit a copy of the document to the user's computer. When the server sends the document to the user's computer for viewing, a transfer of information from the website owner to the user has occurred. Although the website owner's document does not go directly or immediately to the user, once a user accesses a website, information is transferred from the website owner to the user via one of the specified mediums. We therefore conclude that Konop's website fits the definition of "electronic communication."

The Wiretap Act, however, prohibits only "interceptions" of electronic communications. "Intercept" 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." *Id.* § 2510(4). Standing alone, this definition would seem to suggest that an individual "intercepts" an electronic communication merely by "acquiring" its contents, regardless of when or under what circumstances the acquisition occurs. Courts, however, have clarified that Congress intended a narrower definition of "intercept" with regard to electronic communications.

In *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), the Fifth Circuit held that the government's acquisition of email messages stored on an electronic bulletin board system, but not yet retrieved by the intended recipients, was not an "interception" under the Wiretap Act. The court observed that, prior to the enactment of the ECPA, the word "intercept" had been interpreted to mean the acquisition of a communication contemporaneous with transmission. *Id.* at 460 (*citing United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976)). The court further observed that Congress, in passing the ECPA, intended to retain the previous definition of "intercept" with respect to wire and oral communications, while amending the Wiretap Act to cover interceptions of electronic communications. *See Steve Jackson Games*, 36 F.3d at 462; S. Rep. No. 99-541, at 13; H.R. Rep. No. 99-647, at 34. The court reasoned, however, that the word "intercept" could not describe the exact same conduct with respect to wire and electronic communications, because wire and electronic communications were defined

---

disseminate this information to anyone other than those specifically named and allowed here will be banned from this website and held liable to prosecution for violation of the terms and conditions of use and for violation of this contract.

differently in the statute. Specifically, the term "wire communication" was defined to include storage of the communication, while "electronic communication" was not.[5] The court concluded that this textual difference evidenced Congress' understanding that, although one could "intercept" a *wire* communication in storage, one could not "intercept" an *electronic* communication in storage:

> Critical to the issue before us is the fact that, unlike the definition of "wire communication," the definition of "electronic communication" does not include electronic storage of such communications. ... Congress' use of the word "transfer" in the definition of "electronic communication," and its omission in that definition of the phrase "any electronic storage of such communication" ... reflects that Congress did not intend for "intercept" to apply to "electronic communications" when those communications are in "electronic storage."

Steve Jackson Games, 36 F.3d at 461-62; *Wesley Coll. v. Pitts*, 974 F. Supp. 375, 386 (D. Del. 1997) ("By including the electronic storage of wire communications within the definition of such communications but declining to do the same for electronic communications ... Congress sufficiently evinced its intent to make acquisitions of electronic communications unlawful under the Wiretap Act only if they occur contemporaneously with their transmissions."), *aff'd*, 172 F.3d 861 (3d Cir. 1998); *United States v. Reyes*, 922 F. Supp. 818, 836 (S.D.N.Y. 1996) ("Taken together, the definitions thus imply a requirement that the acquisition of [electronic communications] be simultaneous with the original transmission of the data."); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236-37 (D. Nev. 1996) (requiring acquisition during transmission). The *Steve Jackson* Court further noted that the ECPA was deliberately structured to afford electronic communications *in storage* less protection than other forms of communication. *See Steve Jackson Games*, 36 F.3d at 462-64.

The Ninth Circuit endorsed the reasoning of *Steve Jackson Games* in *United States v. Smith*, 155 F.3d at 1051. The question presented in *Smith* was whether the Wiretap Act covered wire communications in storage, such as voicemail messages, or just wire communications in transmission, such as ongoing telephone conversations. Relying on the same textual distinction as the Fifth Circuit in *Steve Jackson Games*, we concluded that wire communications in storage could be "intercepted" under the Wiretap Act. We found that Congress' inclusion of storage in the definition of "wire communication" militated in favor of a broad definition of the term "intercept" with respect to wire communications, one that included acquisition of a communication subsequent to transmission. We further observed that, *with respect to wire communications only*, the prior definition of "intercept" - acquisition contemporaneous with transmission - had been overruled by the ECPA. *Smith*, 155 F.3d at 1057 n. 11. On the other hand, we suggested that the narrower definition of "intercept" was still appropriate with regard to electronic communications:

---

[5] Until October 2001, "wire communication" was defined as "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 ... and *such term includes any electronic storage of such communication* ...." 18 U.S.C. § 2510(1) (2000) (emphasis added).

> In cases concerning "electronic communications" - the definition of which specifically includes "transfers" and specifically excludes "storage" - the "narrow" definition of "intercept" fits like a glove; it is natural to except non-contemporaneous retrievals from the scope of the Wiretap Act. In fact, a number of courts adopting the narrow interpretation of "interception" have specifically premised their decisions to do so on the distinction between § 2510' s definitions of wire and electronic communications.

Smith, 155 F.3d at 1057 (citations and alterations omitted).

We agree with the *Steve Jackson* and *Smith* courts that the narrow definition of "intercept" applies to electronic communications. Notably, Congress has since amended the Wiretap Act to eliminate storage from the definition of wire communication, *see* USA PATRIOT Act § 209, 115 Stat. at 283, such that the textual distinction relied upon by the *Steve Jackson* and *Smith* courts no longer exists. This change, however, supports the analysis of those cases. By eliminating storage from the definition of wire communication, Congress essentially reinstated the pre-ECPA definition of "intercept" - acquisition contemporaneous with transmission - with respect to wire communications. *See Smith*, 155 F.3d at 1057 n. 11. The purpose of the recent amendment was to reduce protection of voice mail messages to the lower level of protection provided other electronically stored communications. *See* H.R. Rep. 107-236(I), at 158-59 (2001). When Congress passed the USA PATRIOT Act, it was aware of the narrow definition courts had given the term "intercept" with respect to electronic communications, but chose not to change or modify that definition. To the contrary, it modified the statute to make that definition applicable to voice mail messages as well. Congress, therefore, accepted and implicitly approved the judicial definition of "intercept" as acquisition contemporaneous with transmission.

We therefore hold that for a website such as Konop's to be "intercepted" in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage.[6] This conclusion is consistent with the ordinary meaning of "intercept," which is "to stop, seize, or interrupt in progress or course before arrival." *Webster's Ninth New Collegiate Dictionary* 630 (1985). More importantly, it is consistent with the structure of the ECPA, which created the SCA for the express purpose of addressing "access to *stored*

---

[6] The dissent, amici, and several law review articles argue that the term "intercept" must apply to electronic communications in storage because storage is a necessary incident to the transmission of electronic communications. *See, e.g.*, Akamine, *supra*, at 561-65; Jarrod J. White, *E-Mail@ Work. Com: Employer Monitoring of Employee E-Mail*, 48 Ala. L. Rev. 1079, 1083 (1997). Email and other electronic communications are stored at various junctures in various computers between the time the sender types the message and the recipient reads it. In addition, the transmission time of email is very short because it travels across the wires at the speed of light. It is therefore argued that if the term "intercept" does not apply to the *en route* storage of electronic communications, the Wiretap Act's prohibition against "intercepting" electronic communications would have virtually no effect. While this argument is not without appeal, the language and structure of the ECPA demonstrate that Congress considered and rejected this argument. Congress defined "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof," 18 U.S.C. § 2510(17)(A), indicating that Congress understood that electronic storage was an inherent part of electronic communication. Nevertheless, as discussed above, Congress chose to afford stored electronic communications less protection than other forms of communication.

... electronic communications and transactional records." S. Rep. No. 99-541 at 3 (emphasis added). The level of protection provided stored communications under the SCA is considerably less than that provided communications covered by the Wiretap Act. Section 2703(a) of the SCA details the procedures law enforcement must follow to access the contents of stored electronic communications, but these procedures are considerably less burdensome and less restrictive than those required to obtain a wiretap order under the Wiretap Act. *See Steve Jackson Games*, 36 F.3d at 463. Thus, if Konop's position were correct and acquisition of a stored electronic communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the SCA. Congress could not have intended this result. As the Fifth Circuit recognized in *Steve Jackson Games*, "it is most unlikely that Congress intended to require law enforcement officers to satisfy the more stringent requirements for an intercept in order to gain access to the contents of stored electronic communications." *Id.; see also Wesley Coll.*, 974 F. Supp. at 388 (same).

Because we conclude that Davis' conduct did not constitute an "interception" of an electronic communication in violation of the Wiretap Act, we affirm the district court's grant of summary judgment against Konop on his Wiretap Act claims.

C. Stored Communications Act

Konop also argues that, by viewing his secure website, Davis accessed a stored electronic communication without authorization in violation of the SCA. The SCA makes it an offense to "intentionally access[]without authorization a facility through which an electronic communication service is provided ... and thereby obtain[]... access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a)(1). The SCA excepts from liability, however, "conduct authorized ... by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c)(2). The district court found that the exception in § 2701(c)(2) applied because Wong and Gardner consented to Davis' use of Konop's website. It therefore granted summary judgment to Hawaiian on the SCA claim.

The parties agree that the relevant "electronic communications service" is Konop's website, and that the website was in "electronic storage." In addition, for the purposes of this opinion, we accept the parties' assumption that Davis' conduct constituted "access without authorization" to "a facility through which an electronic communication service is provided."

We therefore address only the narrow question of whether the district court properly found Hawaiian exempt from liability under § 2701(c)(2). Section 2701(c)(2) allows a person to authorize a third party's access to an electronic communication if the person is 1) a "user" of the "service" and 2) the communication is "of or intended for that user." *See* 18 U.S.C. § 2701(c)(2). A "user" is "any person or entity who - (A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13).

The district court concluded that Wong and Gardner had the authority under § 2701(c)(2) to consent to Davis' use of the website because Konop put Wong and Gardner

on the list of eligible users. This conclusion is consistent with other parts of the Wiretap Act and the SCA which allow intended recipients of wire and electronic communications to authorize third parties to access those communications. In addition, there is some indication in the legislative history that Congress believed "addressees" or "intended recipients" of electronic communications would have the authority under the SCA to allow third parties access to those communications. *See* H.R. Rep. No. 99-647, at 66-67 (explaining that "an addressee [of an electronic communication] may consent to the disclosure of a communication to any other person" and that "[a] person may be an 'intended recipient' of a communication ... even if he is not individually identified by name or otherwise").

Nevertheless, the plain language of § 2701(c)(2) indicates that only a "user" of the service can authorize a third party's access to the communication. The statute defines "user" as one who 1) *uses* the service and 2) is duly authorized to do so. Because the statutory language is unambiguous, it must control our construction of the statute, notwithstanding the legislative history. *See United States v. Daas*, 198 F.3d 1167, 1174 (9th Cir. 1999). The statute does not define the word "use," so we apply the ordinary definition, which is "to put into action or service, avail oneself of, employ." *Webster's* at 1299; *see Daas*, 198 F.3d at 1174 ("If the statute uses a term which it does not define, the court gives that term its ordinary meaning.").

Based on the common definition of the word "use," we cannot find any evidence in the record that Wong ever used Konop's website. There is some evidence, however, that Gardner may have used the website, but it is unclear when that use occurred. At any rate, the district court did not make any findings on whether Wong and Gardner actually used Konop's website - it simply assumed that Wong and Gardner, by virtue of being eligible to view the website, could authorize Davis' access. The problem with this approach is that it essentially reads the "user" requirement out of § 2701(c)(2). Taking the facts in the light most favorable to Konop, we must assume that neither Wong nor Gardner was a "user" of the website at the time he authorized Davis to view it. We therefore reverse the district court's grant of summary judgment to Hawaiian on Konop's SCA claim….

Reinhart, J. dissenting:

…To read a contemporaneity requirement into the definition of "intercept" renders the prohibition against the electronic communication interception largely superfluous, and violates the precept against interpreting one provision of a statute to negate another. Intercept of electronic communications is defined as any "acquisition of the contents of any ... electronic ... communication through the use of any ... device." 18 U.S.C. § 2510 (4). The nature of electronic communication is that it spends infinitesmal amounts of time "en route," unlike a phone call. Therefore, in order to "intercept" an electronic communication, one ordinarily obtains one of the copies made en route or at the destination. These copies constitute "stored electronic communications," as acknowledged by the majority. 18 U.S.C. § 2510(17)(A) ("'electronic storage' means ... any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"). If intercept is defined as solely contemporaneous acquisition, then in contravention of Congressional intent, at most all acquisitions of the contents of electronic communications would escape the intercept prohibition entirely. Jarrod J. White, Commentary, E-Mail@ Work. Com: Employer Monitoring of Employee

E-Mail, 48 *Ala. L. Rev*. 1079, 1083 (1997) ("Following the Fifth Circuit's rationale, [and excluding stored electronic communications from the intercept prohibition] there is only a narrow window during which an E-mail interception may occur - the seconds or milliseconds before which a newly composed message is saved to any temporary location following a send command. Therefore, ... [assuming that stored communications are excluded from the intercept prohibition], interception of E-mail within the prohibition of the ECPA is virtually impossible.")….

[A] reading of the Wiretap Act that includes stored electronic communications in the statute's "intercept" prohibition is consistent with the nature of the technology at issue, leaves no unexplained statutory gaps, and renders none of the myriad provisions of either the Wiretap Act or the Stored Communications Act superfluous. Under such a reading, the Wiretap Act would prohibit the interception of electronic communications, both stored and en route, and subject violators to serious penalties. It would permit law enforcement to intercept such communications using a court order as indicated in § 2516. (Whether or not it would preserve the use of other less savory techniques is a matter this court is not called upon to decide.) A court order can be obtained by state prosecutors in connection with any one of a number of enumerated crimes, and by any assistant United States attorney for the investigation of any federal felony. Wire communications are treated similarly with only minor exceptions (for example, authorization to intercept wire communications is only available for a finite, though extensive, list of federal crimes); this reading, consistent with Congressional intent as revealed in the legislative history of the statute, rejects the idea that stored electronic communications are afforded a lesser degree of protection from interception than stored wire communications.[2]

Comments and Questions

1. How, if at all, should Congress amend ECPA to provide an appropriate degree of protection to electronic communications? Do you agree with the majority or dissent about the interpretation that should be given to the term "intercept"?

2. Critics of a firm, particularly employees, may prefer to post disparaging remarks pseudonymously or anonymously as an alternative to hosting a password-protected website, as Konop did. This strategy may broaden the audience for the critique. However, it does not ensure that the identities of the posters will necessarily be protected against disclosure since identity information is generally accessible through the posters' Internet service or access provider.

[2] In its interpretation of the term "intercept," the majority relies in part on legislative history from the USA Patriot Act. As the Supreme Court has cautioned, however, "'the views of a subsequent Congress form a hazardous basis for inferring the intent of an earlier one.' " *Consumer Prod. Safety Comm'n v. GTE Sylvania, Inc.*, 447 U.S. 109, 117, 64 L. Ed. 2d 766, 100 S. Ct. 2051 (1980)(quoting *United States v. Price*, 361 U.S. 304, 313, 4 L. Ed. 2d 334, 80 S. Ct. 326 (1960). Such subsequent legislative history will "rarely override a *reasonable interpretation* of a statute that can be gleaned from its language and legislative history prior to its enactment." 447 U.S. at 118 n. 13 (emphasis added).