Internet Law: Spring 2010
Professor Grimmelmann
New York Law School

Reading Packet 3

Privacy

Contents

18 U.S.C. § 2510
Definitions

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

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

. . .

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

. . .

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

. . .

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

. . .

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

. . .

(17) "electronic storage" means—

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

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

. . .

18 U.S.C. § 2511

Interception and disclosure of wire, oral, or electronic communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

. . .

shall be punished as provided in subsection (4) . . . .

(2)

(a)

(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

. . .

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

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

. . .

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public . . . .

. . .

18 U.S.C. § 2518
Procedure for interception of wire, oral, or electronic communications

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information: . . . .

. . .

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications . . . if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;

(b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

. . .

18 U.S.C. § 2701
Unlawful access to stored communications

(a) Offense.— Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

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

. . .

(c) Exceptions.— Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

18 U.S.C. § 2702
Voluntary disclosure of customer communications or records

(a) Prohibitions.— Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

. . .

(3) a provider of . . . electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) . . .) to any governmental entity.

(b) Exceptions for disclosure of communications.— A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511 (2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

. . .

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) Exceptions for Disclosure of Customer Records.— A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service . . .—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

. . . [or]

(6) to any person other than a governmental entity.

18 U.S.C. § 2703
Required disclosure of customer communications or records

(a) Contents of Wire or Electronic Communications in Electronic Storage.— A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Wire or Electronic Communications in [an electronic communication service].—

(1) A governmental entity may require a provider of [electronic communication service] to disclose the contents of any wire or electronic communication [held in electronic storage for more than 180 days]—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

. . .

(c) Records Concerning Electronic Communication Service . . .—

(1) A governmental entity may require a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

. . .

(C) has the consent of the subscriber or customer to such disclosure;

. . . [or]

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service . . . shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number)

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for Court Order.— A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter.— No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

. . .

CLASS 13: ANONYMITY

The challenges of litigating cases about online speech give us a good transition into our discussion of privacy. If the intermediary is immune from suit under Section 230, the victim's only recourse is against the original poster. But to sue someone, you need to know whom to sue. Thus, the seemingly procedural law governing the "unmasking" of Internet users takes on central importance—it may as significant and as controversial as the substantive law to be applied. Interwoven with this story of *private* unmasking is a related set of issues related to *governmental* unmasking of Internet users, primarily during criminal investigations. Our materials today (and through the rest of the privacy unit) will jump back and forth between these two settings. Ask yourself how the policy issues they raise are similar, and how they are different.

Preparation questions

(1) We start with a passage from Vernor Vinge's novella *True Names*, one of the classics in the canon of cyberspace literature. (It's fair to say that many people in the computer industry had their early vision of the Internet and virtual reality shaped by Vinge's book, which also influenced policy debates in the 1990s.) This section is from early on, so there are no big spoilers. Who is Mr. Slippery? Who is the Great Enemy, and why does it have that name? What kinds of harms could Mr. Slippery cause as long as his True Name was unknown? What are the dangers to Roger Pollack once his online pseudonym becomes known? Do these facts explain why the politics of online identifiability are so explosively controversial?

(2) We start our legal analysis on the civil side. I've given you a later ruling from the AutoAdmit case, discussed last time. Note the case caption: *Doe v. Individuals*. The plaintiffs are attempting to proceed anonymously, while asking the court to reveal publicly the identities of the defendants. Is this fair? Why does each side desire pseudonymity? (While we're at it, what's the difference between anonymity and pseudonymity?) What are the advantages of being pseudonymous, and which of these are good for society?

(3) Here, one of the defendants is seeking to quash a subpoena to identify him. This introduces an important point of civil practice. A subpoena is a court order demanding that the recipient appear or produce specified documents. But subpoenas aren't subject to judicial oversight before they issue. *See* Fed. R. Civ. Proc. 45(a)(3)("The clerk must issue a subpoena, signed but otherwise in blank, to a party who requests it. That party must complete it before service.") Instead, the proper response from the recipient of an improper subpoena is a motion to *quash* (not "squash") it. In *Doe v. Individuals*, Doe 21 has filed the motion to quash. That's interesting: the subpoena was actually issued to AT&T. Why didn't AT&T move to quash? Could it have? How did Doe 21 find out about the subpoena?

(4) The next big question in *Doe v. Individuals* is the standard the court should use in deciding whether the plaintiffs have made an "adequate showing as to their claims against the anonymous defendant." Civil procedure gives us plenty of familiar standards. For example, the court could use a motion to dismiss standard: has the plaintiff pleaded all the elements of a valid cause of action? What's wrong with this standard; what harms would result if courts consistently used it when deciding to unmask defendants? Or, perhaps, the court could use a summary judgment standard: the plaintiff must introduce sufficient evidence to prove every element of her claim. What's wrong with this standard? In a deeper sense, why are unmasking subpoenas hard for courts to deal with? Courts are usually pretty good at fact-

finding; what's missing in a John Doe case that makes the task significantly harder? What standard does the court settle on? How good a job do you think it does at balancing the relevant interests?

(5) These rules give us a new perspective on Section 230. Consider first the well-meaning web site that wants to offer a useful service while also protecting people from harm. How do the rules on permissive and mandatory disclosure of user identity affect what this well-meaning site will do? Next consider the indifferent web site: it will do whatever is the least work. How will it behave in response to its incentives under Section 230 and privacy law? Finally, think about the malicious web site: it wants to help its users behave badly without getting into legal trouble itself. How will it behave? Keep in mind that most web servers are by default configured to retain "server logs," which contain the time of each request for a web page, the IP address of the requesting computer, and the URL of the requested page, among other things.

(6) Finally, some statute reading. I've given you a number of sections from the Wiretap Act and the Stored Communications Act. I've tried to prune the thicket as much as possible, but the part that remains still has brambles, and you'll need to make your way through it.[1] The basic rule on disclosing the identity of an user is set forth in 18 U.S.C. § 2702(a)(3). Go look it up now. Now suppose that you work for Hotmail. You have just received a letter from the NYPD requesting the real name, address, and any other relevant contact information of the user with email address "ThinBlueLiar@hotmail.com." How should you respond? Why? What if the letter came from the Whole Foods corporation instead? Be sure to consult the definitions in § 2510 and the list of exceptions in § 2702(c).

(7) This basic rule governs voluntary disclosures. A second rule deals with *required* disclosures. *See* §§ 2703(c)–(e). If you work for the NYPD and you want to compel Hotmail to disclose the subscriber information for ThinBlueLiar, can you, and if so, how? What if you work for Whole Foods? What justifies the different treatment of governmental and private entities?

BLOWN TO BITS, ch. 7

Please read chapter 7 of *Blown to Bits*.

VERNOR VINGE, TRUE NAMES (1981)

In the once upon a time days of the First Age of Magic, the prudent sorcerer regarded his own true name as his most valued possession but also the greatest threat to his continued good health, for—the stories go—once an enemy, even a weak unskilled enemy, learned the sorcerer's true name, then routine and widely known spells could destroy or enslave even the most powerful. As times passed, and we graduated to the Age of Reason and thence to the first and second

[1] In particular, if you are going to do any work on the criminal side that touches on computers or the Internet, you'll need to learn a great deal about these privacy statutes. I recommend Orin Kerr's *Computer Crime Law*, which is half casebook and half treatise, as an introduction.

industrial revolutions, such notions were discredited. Now it seems that the Wheel has turned full circle (even if there never really was a First Age) and we are back to worrying about true names again:

The first hint Mr. Slippery had that his own True Name might be known—and, for that matter, known to the Great Enemy—came with the appearance of two black Lincolns humming up the long dirt driveway that stretched through the dripping pine forest down to Road 29. Roger Pollack was in his garden weeding, had been there nearly the whole morning, enjoying the barely perceptible drizzle and the overcast, and trying to find the initiative to go inside and do work that actually makes money. He looked up the moment the intruders turned, wheels squealing, into his driveway. Thirty seconds passed, and the cars came out of the third-generation forest to pull up beside and behind Pollack's Honda. Four heavy-set men and a hard-looking female piled out, started purposefully across his well-tended cabbage patch, crushing tender young plants with a disregard which told Roger that this was no social call.

Pollack looked wildly around, considered making a break for the woods, but the others had spread out and he was grabbed and frog-marched back to his house. (Fortunately the door had been left unlocked. Roger had the feeling that they might have knocked it down rather than ask him for the key.) He was shoved abruptly into a chair. Two of the heaviest and least collegiate-looking of his visitors stood on either side of him. Pollack's protests—now just being voiced—brought no response. The woman and an older man poked around among his sets. "Hey, I remember this, Al: It's the script for 1965. See?" The woman spoke as she flipped through the holo-scenes that decorated the interior wall.

The older man nodded. "I told you. He's written more popular games than any three men and even more than some agencies. Roger Pollack is something of a genius."

They're novels, damn you, not games! Old irritation flashed unbidden into Roger's mind. Aloud: "Yeah, but most of my fans aren't as persistent as you all." "Most of your fans don't know that you are a criminal, Mr. Pollack."

"Criminal? I'm no criminal—but I do know my rights. You FBI types must identify yourselves, give me a phone call, and—"

The woman smiled for the first time. It was not a nice smile. She was about thirty-five, hatchet-faced, her hair drawn back in the single braid favored by military types. Even so it could have been a nicer smile. Pollack felt a chill start up his spine. "Perhaps that would be true, if we were the FBI or if you were not the scum you are. But this is a Welfare Department bust, Pollack, and you are suspected—putting it kindly—of interference with the instrumentalities of National and individual survival." . . .

"Look, in spite of what you may want, all this is still legal. In fact, that gadget is scarcely more powerful than an ordinary games interface." That should be a good explanation, considering that he was a novelist.

The older man spoke almost apologetically, "I'm afraid Virginia has a tendency to play cat and mouse, Mr. Pollack. You see, we know that in the Other World you are Mr. Slippery." "Oh." There was a long silence. Even "Virginia" kept her mouth shut. This had been, of course, Roger Pollack's great fear. They had discovered Mr. Slippery's True Name and it was Roger Andrew

Pollack TIN/SSAN 0959-34-2861, and no amount of evasion, tricky programming, or robot sources could ever again protect him from them.

Doe I and Doe II v. Individuals, whose true names are unknown
561 F. Supp. 2d 249 (D. Conn. 2008)

CHRISTOPHER F. DRONEY, District Judge.

On February 1, 2008, the plaintiffs, Jane Doe I and Jane Doe II (the "Does") issued a subpoena *duces tecum* to SBC Internet Services, Inc., now known as AT & T Internet Services ("AT & T"), the internet service provider, for information relating to the identity of the person assigned to the Internet Protocol ("IP") address from which an individual using the pseudonym "AK47" posted comments on a website. The individual whose internet account is associated with the IP address at issue, 251 referring to himself as John Doe 21,[1] has moved to quash that subpoena. John Doe 21 has also moved for permission to proceed anonymously in this matter.

I. Background

This action was brought by Doe I and Doe II, both female students at Yale Law School, against unknown individuals using thirty-nine different pseudonymous names to post on a law school admissions website named AutoAdmit.com ("AutoAdmit"). The plaintiffs allege that they were the targets of defamatory, threatening, and harassing statements posted on AutoAdmit from 2005 to 2007.

[The relevant facts are set forth in the complaint in *Doe v. Ciolli*, which you read for last time and may treat as true for the purposes of today's discussion. But query whether this is the correct legal standard. Should the court engage in fact-finding? If so, where else should it look for relevant information?]

. . . The news of the filing of the Does' complaint quickly became a subject of discussion on AutoAdmit. AK47, for example, wrote a post concerning his opinion on the merits of the plaintiffs' case, and wondered whether posters were "allowed to use [Doe II's] name in thread's anymore." Subsequently, on June 17, 2007, AK47 posted the statement "Women named Jill and Doe II should be raped." On June 24, 2007, AK47 started a thread entitled "Inflicting emotional distress on cheerful girls named [Doe II]."

On February 1, 2008, the plaintiffs issued a subpoena *duces tecum* to AT & T for information relating to the identity of the person assigned to the IP address from which an individual using the pseudonym "AK47" posted comments on AutoAdmit about Doe II. This subpoena was issued in accordance with this Court's order of January 29, 2008, which granted the Does' motion to engage in limited, expedited discovery to uncover the identities of the defendants in this case. On February 7, 2008, AT & T sent a letter to the person whose internet account corresponded with the IP address at issue, John Doe 21 ("Doe 21"), notifying Doe 21 that it had received a subpoena ordering it to produce certain information relating to Doe 21's internet account. The letter stated that Doe 21 could file a motion to quash or for a protective order before the date of production, which was February 25, 2008, and that AT & T must receive a

---

[1] Because John Doe 21 chose a male pseudonymous name to proceed under, the Court will refer to John Doe 21 using male pronouns. This does not reflect a finding by the Court that John Doe 21 is indeed male.

copy of such a motion prior to that date. Doe 21 filed the instant motion to quash on February 25, 2008, and on February 26, 2008, A & T complied with the subpoena. On March 12, 2008, Doe 21 filed his motion to proceed anonymously.

Because Doe 21 does not have counsel and his true identity is yet unknown to the Court, the Court appointed pro bono counsel to represent the interests of Doe 21 at oral argument on the instant motions, which took place on May 5, 2008.

II. Motion to Quash

A. Threshold Issues

. . .

2. Mootness

Doe II argues that the motion to quash is moot because the information sought has already been turned over to the plaintiffs by AT & T. However, the Court rejects this argument because the plaintiffs can be ordered to return the information and be prohibited from using it. *See Sony Music Entertainment Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 561 (S.D.N.Y. 2004).

B. Merits of the Motion to Quash

A subpoena shall be quashed if it "requires disclosure of privileged or other protected matter and no exception or waiver applies." Fed.R.Civ.P. 45(c)(3)(A)(iii). Doe 21 moves to quash the subpoena because he claims disclosure of his identity would be a violation of his First Amendment right to engage in anonymous speech.

The First Amendment generally protects anonymous speech. The United States Supreme Court has also made clear that the First Amendment's protection extends to speech on the internet. Courts also recognize that anonymity is a particularly important component of Internet speech. "Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas[;] ... the constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded." *Doe v. 2TheMart.com Inc.*, 140 F. Supp.2d 1088, 1092, 1097 (W.D.Wash.2001). However, the right to speak anonymously, on the internet or otherwise, is not absolute and does not protect speech that otherwise would be unprotected. *See, e.g.*, . . . *In re Subpoena Duces Tecum to America Online, Inc.*, No. 40570, 2000 WL 1210372, at *6 (Va.Cir.Ct. 2000) ("Those who suffer damages as a result of tortious or other actionable communications on the Internet should be able to seek appropriate redress by preventing the wrongdoers from hiding behind an illusory shield of purported First Amendment rights."). . . .

The forgoing principles and decisions make clear that Doe 21 has a First Amendment right to anonymous Internet speech, but that the right is not absolute and must be weighed against Doe II's need for discovery to redress alleged wrongs. Courts have considered a number of factors in balancing these two competing interests: This balancing analysis ensures that the First Amendment rights of anonymous Internet speakers are not lost unnecessarily, and that plaintiffs do not use discovery to "harass, intimidate or silence critics in the public forum opportunities presented by the Internet." *Dendrite Intern. Inc. v. Doe No. 3*, 342 N.J.Super. 134, 775 A.2d 756, 771 (2001). The Court will address each factor in turn.

First, the Court should consider whether the plaintiff has undertaken efforts to notify the anonymous posters that they are the subject of a subpoena and withheld action to afford the fictitiously named defendants a reasonable opportunity to file and serve opposition to the application. . . . In this case, the plaintiffs have satisfied this factor by posting notice regarding the subpoenas on AutoAdmit in January of 2008, which allowed the posters ample time to respond, as evidenced by Doe 21's activity in this action.

Second, the Court should consider whether the plaintiff has identified and set forth the exact statements purportedly made by each anonymous poster that the plaintiff alleges constitutes actionable speech. Doe II has identified the allegedly actionable statements by AK47/ Doe 21: the first such statement is "Alex Atkind, Stephen Reynolds, 255 [Doe II], and me: GAY LOVERS;" and the second such statement is "Women named Jill and Doe II should be raped." The potential liability for at least the first statement is more fully discussed below.

The Court should also consider the specificity of the discovery request and whether there is an alternative means of obtaining the information called for in the subpoena. Here, the subpoena sought, and AT & T provided, only the name, address, telephone number, and email address of the person believed to have posted defamatory or otherwise tortious content about Doe II on AutoAdmit, and is thus sufficiently specific. Furthermore, there are no other adequate means of obtaining the information because AT & T's subscriber data is the plaintiffs' only source regarding the identity of AK47.

Similarly, the Court should consider whether there is a central need for the subpoenaed information to advance the plaintiffs' claims. Here, clearly the defendant's identity is central to Doe II's pursuit of her claims against him.

Next, the Court should consider the subpoenaed party's expectation of privacy at the time the online material was posted. Doe 21's expectation of privacy here was minimal because AT & T's Internet Services Privacy Policy states, in pertinent part: "We may, where permitted or required by law, provide personal identifying information to third parties ... without your consent ... To comply with court orders, subpoenas, or other legal or regulatory requirements." Thus, Doe 21 has little expectation of privacy in using AT & T's service to engage in tortious conduct that would subject him to discovery under the federal rules.

Finally, and most importantly, the Court must consider whether the plaintiffs have made an adequate showing as to their claims against the anonymous defendant. Courts have differed on what constitutes such an adequate showing. Several courts have employed standards fairly deferential to the plaintiff, requiring that the plaintiff show a "good faith basis" to contend it may be the victim of conduct actionable in the jurisdiction where the suit was filed; or to show that there is probable cause for a claim against the anonymous defendant. The Court finds these standards set the threshold for disclosure too low to adequately protect the First Amendment rights of anonymous defendants, and thus declines to follow these approaches.

Other courts have required that a plaintiff show its claims can withstand a motion to dismiss. However, other courts have rejected this procedural label as potentially confusing because of the variations in the motion to dismiss standard in different jurisdictions. Similarly, but more burdensome, some courts have used a standard which required plaintiffs to show their claims could withstand a motion for summary judgment. The Court finds this standard to be both potentially confusing and also difficult for a plaintiff to satisfy when she has been unable to

conduct any discovery at this juncture. Indeed, it would be impossible to meet this standard for any cause of action which required evidence within the control of the defendant.

Several courts have required that a plaintiff make a concrete showing as to each element of a prima facie case against the defendant. Under such a standard, "[w]hen there is a factual and legal basis for believing [actionable speech] has occurred, the writer's message will not be protected by the First Amendment." The Court finds such a standard strikes the most appropriate balance between the First Amendment rights of the defendant and the interest in the plaintiffs of pursuing their claims, ensuring that the plaintiff "is not merely seeking to harass or embarrass the speaker or stifle legitimate criticism."

Doe II has presented evidence constituting a concrete showing as to each element of a prima facie case of libel against Doe 21. Libel is written defamation. To establish a prima facie case of defamation under Connecticut law, the Doe II must demonstrate that: (1) Doe 21 published a defamatory statement; (2) the defamatory statement identified the plaintiff to a third person; (3) the defamatory statement was published to a third person; and (4) the plaintiffs reputation suffered injury as a result of the statement.

A defamatory statement is defined as a communication that tends to "harm the reputation of another as to lower him in the reputation of the community or to deter third persons from associating or dealing with him . . ." . . . Doe II alleges, and has presented evidence tending to show that, AK47's statement, "Alex Atkind, Stephen Reynolds, [Doe II], and me: GAY LOVERS," is defamatory, because any discussion of Doe II's sexual behavior on the internet tends to lower her reputation in the community, particular in the case of any potential employers who might search for her name online.[1] In fact, in the similar context of slander (spoken defamation), any statement that imputes "serious sexual misconduct" to a person subjects the publisher to liability, without any need to prove the special harms required for other slanderous speech.

Doe II has also alleged and presented evidence that Doe 21's statement clearly identified Doe II by name and was available to a large number of third persons (peers, colleagues, potential employers), whether they were on Autoadmit for their own purposes, or searched for Doe II via a search engine. Finally, Doe II has alleged and provided evidence that her reputation did suffer injury because of this comment. In her interviews with potential employers in the Fall of 2007, Doe II felt she needed to disclose that existence of this and other such comments on AutoAdmit and explain that she had been targeted by pseudonymous online posters. In addition, this statement has contributed to difficulties in Doe II's relationships with her family, friends, and classmates at Yale Law School.

Thus, the plaintiff has shown sufficient evidence supporting a prima facie case for libel, and thus the balancing test of the plaintiff's interest in pursuing discovery in this case outweighs the

---

[1] Context is relevant in determining the meaning of a statement. See 3 Restatement (Second), Torts 563, at 163. Doe 21 suggests that the context in which the statements were made also shows that they were not defamatory, because AutoAdmit is well-known as a place for inane discussion and meaningless derogatory postings, such that one would not take such a statement seriously. However, not everyone who searched for Doe II's name on the internet, or who came across the postings on AutoAdmit, would be aware of the site's alleged reputation. Thus, Doe II has put forth sufficient evidence for a prima facie case of defamation.

defendant's First Amendment right to speak anonymously. The defendant's motion to quash is denied. . . .

Cohen v. Google problem

This problem is based on actual facts, as described in *Cohen v. Google*, 25 Misc.3d 945 (N.Y. Sup. Ct. 2009), *available at* http://m.mediapost.com/pdf/Cohen_doc.pdf, and in various news stories, such as Lachlan Cartwright et al., *Secret Grudge of NY 'Skankies'*, N.Y. POST, Sept. 2, 2009, *available at* http://www.nypost.com/p/news/regional/item_f6c4ttnK4zchSR51tDJoYJ.

Liskula Cohen is a fashion model who lives in New York. On August 21, 2008, an unknown party created blog on Google's Blogspot blog hosting service called "Skanks of NYC." It contained five posts. Here's a sampling:

> I would have to say that the first place award for "Skankiest in NYC" would have to go to Liskula Gentile Cohen. How old is this skank? 40 something? She's a psychotic, lying, whoring, still going to clubs at her age, skank. . . .
>
> Yeah she may have been hot 10 years ago, but is it really attractive to watch this old hag straddle dudes in a nightclub or lounge? Desperation seeps from her soul, if she even has one.

Cohen filed, in the New York Supreme Court, for a court order for "pre-action disclosure" for discovery of the anonymous blogger's identity under N.Y. CPLR § 3102(c), explaining that the information was necessary for Cohen to pursue a defamation lawsuit against the blogger. Google informed the court that it had no substantive objection to the disclosure but had forwarded the request to the blogger. Through counsel, the blogger contested the motion.

(1) **Has Cohen satisfied the standard for disclosure of the blogger's identity?**

In the event, the court granted Cohen's motion. Google disclosed that the anonymous blogger was Rosemary Port, whom Cohen knew socially. Cohen instructed her lawyer to drop the lawsuit.

(2) **Why might Cohen have dropped the lawsuit? Does her decision call into question the court's decision to grant her the requested discovery? What should courts do in situations like this?**

Meanwhile, Port announced that she planned to sue Google for revealing her identity.

(3) **Does Port have a valid cause of action against Google?**

Jukt Micronics problem

You are an Assistant U.S. Attorney assigned to help the FBI investigate a computer intrusion at Jukt Micronics, which designs and manufactures circuit boards for high-performance scientific computing in physics and chemistry labs. Recently, someone has managed to gain access to—and overwrite—a file containing the prototype design for the JK-478, the company's next big project. The file was replaced with a pornographic picture which was captioned, "THE BIG BAD BIONIC BOY HAS BEEN HERE BABY."

This morning, the firm's CEO received an email from eatmyjukt@hiert.com. Hiert.com is an ad-supported web email system: users don't need to supply anything more than a desired username and password to create an account. The email's author, "Ian," claimed to be responsible for the computer intrusion and to have the original file in his possession. He demanded $250 million for its return. The number is so obviously outrageous—Jukt's entire annual revenues are only about $40 million—that you and your FBI contact are starting to suspect you're dealing with a talented and possibly underage amateur, rather than with real industrial espionage.

Leaving aside other possible investigative avenues, how should you attempt to turn "eatmyjukt" into an actual name and address so that the FBI can ask "Ian" some questions? How likely is this process to succeed? What could go wrong? Your strategy should consider both the technical and legal aspects of the problem. (*Hint*: The technical part will take more than one step. The legal part is straightforward, if you do things right.)

CLASS 14: ENCRYPTION

Last class was about your ability to keep your identity confidential while online. Today, we set off into deeper waters: your ability to keep *what you say* confidential while online. We start with the criminal side: under what circumstances can the police (or the FBI, etc.) read your emails and other communications? Answering this question will require us to start learning some constitutional criminal procedure: primarily the Fourth and Fifth Amendments. We'll also talk a bit about statutory regimes, principally the ECPA. Very roughly, this class will be devoted to information you yourself try to hide for yourself; next class will bring third parties into the picture.

Today, in order to give some shape to the topic, we'll focus on *encryption*: the use of computer technology to render messages readable by their intended recipients but not by anyone else. A warning: this is dense material. I'm simplifying enormously—and it will still likely be rough sailing. We'll try to focus on a few key principles and issues. Don't mistake them for the whole of the subject.

Preparation questions

(1) There're a lot of interesting issues in *David*. I suggest that you and a friend act out the scene, with one of you playing David and the other Special Agent Peterson. At each beat in the story, stop and analyze the Fourth Amendment implications of what just happened. Do you see how the court reached the conclusions it did? Were they correct? Was there another, better way the government could have played its hand? What about David? Is there anything he could or should have done differently?

(2) In *David*, the government got past the encryption by surreptitiously observing David's password. (It wasn't a very good password, was it?) This works surprisingly often. In *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001), the FBI broke in to the defendant's office and installed a "key logger" on his computer keyboard that recorded his keystrokes. (The logger was configured to avoid capturing anything he typed while the computer was connected to the Internet, for reasons we'll explore next time.) The FBI thereby obtained the password he used to encrypt his files, which contained evidence of gambling and loansharking. Do you see any constitutional issues with this procedure? If so, how would you carry it out so that the resulting evidence will be admissible in court?

(3) In a sense, Officer Zenobia's "mistake" in the coffeeshop problem is not observing the defendant typing the password into the computer. How much of a mistake is it really, given the circumstances? Often, the defendant is already on the alert, perhaps even in custody. Thus, the challenge shifts to prying the information from an unwilling defendant, either by convincing them to reveal the password, or by using "brute force" to decrypt the message without the password. What Fourth and Fifth Amendment issues do these two routes use?

(4) But don't let the central encryption issue distract you from the *other* issues lurking in the coffeeshop problem. Call back your friend and walk through Officer Zenobia's actions. Does she have a Fourth Amendment justification at each step? What information has she gained that will be legally admissible at trial? What does this evaluation tell you about option (3) in the problem?

(5) The Zipper problem combines legal, technical, and policy issues. Banning the *use* of cryptography obviously raises one set of concerns, but banning the *export* of software raises another. The Senator's office is obviously thinking about devices like Zipper phones—but what does an "export" control on software (which is, after all, just a bunch of bits) mean? From the perspective of software developers and cryptography researchers, is there something troubling about the proposal beyond just the surveillance issues? Key escrow though—that one has to be fine, right? After all, it's a secure government database that can only be opened with a court order and the Zipper communications are completely secure otherwise. How could anything possibly go wrong?

UNITED STATES CONSTITUTION

Amendment IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Amendment V

. . . nor shall any person . . . be compelled in any criminal case to be a witness against himself . . . .

Fourth and Fifth Amendment Overview

Ready? Deep breath. Here we go.

The basic command of the Fourth Amendment, as interpreted by the Supreme Court, is that the government may not "search" you or your private spaces or "seize" you or your physical property unless it has obtained a search warrant. A search warrant is a judicial order that gives the police permission to carry out the search or seizure. It can only be issued by a court after the police provide "probable cause," i.e., "a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). It must also specify which particular places are to be searched, or which items are to be seized; a search or seizure that goes beyond those limits is invalid. A search without a valid warrant is illegal, and the "exclusionary rule" governs any evidence the police obtain as a result: it may not be introduced at trial.

This sounds simple enough. If the police kick down your door and start flipping through your casebooks, that's a search. If they handcuff you, that's a seizure of your person; if they take your gym clothes down to the precinct, that's a seizure of your property. But even before we get to computers, there are complications.

First, not everything is a "search" or a "seizure." If a police officer sees you run out of a bank wearing a ski mask and waving a gun, it's not a "search" for Fourth Amendment purposes in the first place. More generally, unless the governmental action violates your "reasonable expectation of privacy," no search has taken place. This test standard comes from *Katz v. United*

States, 389 U.S. 347 (1967). There, the police bugged a phone booth they knew the defendant regularly used; the Supreme Court held that this constituted a search for which a warrant was required. Drawing the line that defines a "reasonable expectation of privacy" is extremely hard, but a few examples are relatively clear. You have a reasonable expectation of privacy in your home, and in sealed containers, such as suitcases, paper bags, automobile trunks and so on. By contrast, you have no reasonable expectation of privacy in anything you have voluntarily exposed to public view.

"Seizure" is a little easier to define. A seizure of your person is an arrest or other involuntary restriction of your liberty to leave. A seizure of your property takes place when there is "some meaningful interference with [your] possessory interest." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). In the offline world, at least, this is relatively straightforward most of the time.

The second complication is that the Fourth Amendment prohibits only "unreasonable" searches and seizures. A warrantless search could still be "reasonable" and thus permissible. Some of these exceptions (each of which has its own tests) take us well outside the scope of this course—at the U.S. border, in government workplaces, in schools and prisons, and as part of a lawful arrest. The police may also conduct searches and seizures when "exigent circumstances" make obtaining a warrant infeasible—most commonly, when there is a risk that evidence will be destroyed if they do not act.

Two others are important to us. First, there's the "consent" exception: if the suspect or someone else with authority over the property consents, the police may search it. If you invite the police into your basement meth lab, you may not later argue that it was a private space they needed a warrant to enter. The same goes if your housemate invites them into the shared meth lab. The second is the "plain view" rule. If the police are executing a valid search warrant, they may *also* search seize evidence whose incriminating nature is "immediately apparent." If the police are searching the basement meth lab pursuant to a valid warrant, they can also follow the trail of blood up the stairs. These two exceptions have a lot in common with the basic reasonable-expectation-of-privacy test: can you articulate the general principle that unites them?

Now for the Fifth Amendment. We're concerned only with its privilege against self-incrimination, which gives us that wonderful phrase, "taking the Fifth." Not only can the government not force you to testify at your trial, it also cannot force you to to answer police questions. Specifically, the Fifth Amendment protects against "compelled," "incriminating," and "testimonial" communications. They're subject to the exclusionary rule we met above.

It kicks in which the police *compel* you to speak (so voluntary confessions aren't a Fifth Amendment concern), when the communications are used against you in a criminal proceeding (so if you're given a grant of criminal immunity, you *must* answer the questions), and and when they are "testimonial." A communication is "testimonial" when it includes statements of fact. Your diary is testimonial; it includes your statements of what you did and when. (Note that if the police find and seize your diary; its contents may be used against you; they simply can't force you to give it to them or reveal where it is.) But a blood sample is not testimonial; your blood type is just a fact of nature, not something you do or say.

A. Michael Froomkin, *The Metaphor Is the Key*
***Cryptography, The Clipper Chip, and the Constitution*, 143 U. PENN. L. REV. 709 (1995)**

Cryptologists use a few terms that may not be familiar to lawyers, and it is useful to define them at the outset of any discussion relating to encryption. *Cryptography* is the art of creating and using methods of disguising messages, using codes, ciphers, and other methods, so that only certain people can see the real message. Codes and ciphers are not the same. A *code* is a system of communication that relies on a pre-arranged mapping of meanings such as those found in a code book. A *cipher* is a method of encrypting any text regardless of its content. Paul Revere's "[o]ne, if by land, and two, if by sea" was a code. If the British had landed by parachute, no quantity of lanterns would have sufficed to communicate the message. . . .

Those who are supposed to be able to read the message disguised by the code or cipher are called *recipients*. "The original message is called a *plaintext*. The disguised message is called a *ciphertext*. *Encryption* means any procedure to convert plaintext into ciphertext. *Decryption* means any procedure to convert ciphertext into plaintext." An *algorithm* is a more formal name for a cipher. An algorithm is a mathematical function used to encrypt and decrypt a message. Modern algorithms use a *key* to encrypt and decrypt messages. A *single-key* system is one in which both sender and receiver use the same key to encrypt and decrypt messages. Until recently, all ciphers were single- key systems. One of the most important advances in cryptography is the recent invention of *public-key systems*, which are algorithms that encrypt messages with a key that permits decryption only by a different key.

United States v. David
756 F. Supp. 1385 (D. Nev. 1991)

LAWRENCE R. LEAVITT, United States Magistrate Judge.

On June 21, 1990, the federal grand jury returned a one-count Indictment charging the defendant, Artem Bautista David, with conspiracy to import more than 20 kilos of heroin into the United States. . . .

I. *The Evidence*

An evidentiary hearing was conducted before the undersigned Magistrate Judge on September 12, 1990. The testimony established that in late April, 1990, David flew from Hong Kong to Las Vegas and was taken into custody by Customs agents on a charge of conspiracy to smuggle heroin into the United States. Government counsel engaged in discussions with David's then counsel, John R. Lusk, with a view toward enlisting David's cooperation in exchange for a favorable plea bargain. An agreement was reached whereby David, who would remain in custody under a detention order, would meet periodically with the agents in their office and make full disclosure of his knowledge of drug trafficking activities in an "off the record" proffer. . . . The agreement also provided that at the agents' direction, David would place consensually monitored telephone calls to his criminal associates. The telephone numbers of those associates were kept in David's computer memo book, access to which required the use of a password — "fortune" — which was known only to David.

During one such meeting in early May, 1990, which Lusk attended, David retrieved and disclosed certain information contained in the book. At the time, the agents were sitting across

the table from him and were unable to see the password which David used or the information displayed on the book's screen. David did not volunteer the password to the agents, or offer to show them the book.

Jail regulations prohibited David from taking the book back to the jail at night. For the sake of convenience, Lusk permitted the agents to maintain custody of the book at the end of each session. Lusk did not, however, give them permission to access the book. Neither did David. Nor, as noted above, did the assistance agreement itself expressly permit the agents to gain access to the book or, for that matter, to any other property in David's possession.

At the next meeting on May 7, 1990, David met with Customs Special Agent Eric Peterson and DEA Special Agent Don Ware. Lusk did not attend this meeting. According to David's testimony, when he initially accessed the book at this meeting, Agent Peterson got up and stood directly behind him. David was aware that Peterson was looking over his shoulder, but did not feel that he could demand that Peterson move away. David did, however, try to position the book so as to minimize Peterson's view of it.

According to David's testimony, after he made two telephone calls for the agents, Peterson grabbed the book and accused David of deleting certain information. David demanded the book back, but Peterson refused. At the evidentiary hearing, David denied having deleted information from the book. Agent Peterson's version of what occurred at the meeting is a little different. Peterson testified that on May 7, 1990, he first requested the access code from David, but David was unresponsive. Peterson admitted that he then stood behind David and observed David use the password "fortune" to access the book. A little later, while Agent Ware was criticizing David for not cooperating fully during a consensually monitored phone call, Peterson, without requesting David's permission, used the password "fortune" and accessed the book himself. He then reviewed several of its entries. David saw Peterson doing this, but said nothing. Peterson came across an entry which read "1 = 12,000; 2 = 23,000," which, based on his experience as a Customs agent, he knew to be a heroin price list per kilo in Thailand. He then turned off the computer and returned it to David. . . .

II. Discussion

The Fourth Amendment provides that the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated...." The Supreme Court has defined a search as an infringement of "an expectation of privacy that society is prepared to consider reasonable." *United States v. Jacobsen*, 466 U.S. 109, 113, 104 S.Ct. 1652, 1656, 80 L.Ed.2d 85 (1984). Hence, a law enforcement officer who looks at something has not engaged in a "search" within the meaning of the Fourth Amendment unless someone else has a right to expect that the thing which is seen will remain private.

A seizure of tangible property is defined as "some meaningful interference with an individual's possessory interest in that property." Ibid. Therefore, unless an individual's control over or access to property in which he or she has a possessory interest is interrupted or otherwise interfered with by law enforcement officers in some meaningful way, there is no "seizure" within the meaning of the Fourth Amendment. . . .

In evaluating the factual scenario described above, we begin by identifying those events which may have Fourth Amendment implications. The *first* such event occurred when Agent Peterson deliberately looked over David's shoulder to see the password to the book. David himself

voluntarily accessed the book at a time when the agents were in close proximity to him. Agent Peterson was not required to stay seated across the table from David. Nor did David have a reasonable expectation that Peterson would not walk behind him, or remain outside of some imaginary zone of privacy within the enclosed room. It was Peterson's office, and he could move about in it wherever he pleased. The Court therefore finds that under the circumstances David had no reasonable expectation of privacy in the display that appeared on the screen, and accordingly concludes that Peterson's act of looking over David's shoulder to see the password did not constitute a search within the meaning of the Fourth Amendment. . . .

The *second* such event occurred when Peterson picked up the book, turned it on and entered the password. Peterson's use of the book lasted only a few moments, and David was not prevented thereby from using the book himself. Peterson's act of picking up the book was therefore not a seizure, because it did not interfere with David's possessory interest in the book in any meaningful way.

Peterson's act of accessing the book did constitute a search, however, if, under the circumstances, David had a reasonable expectation that when he turned the book off, its contents would remain private. For the purposes of this discussion, the book, in the Court's view, is indistinguishable from any other closed container, and is entitled to the same Fourth Amendment protection. The Court does not question Agent Peterson's testimony that based on David's cooperation agreement with the government, Peterson had a good faith belief that he had the right to access the book. Peterson testified that in his mind the cooperation agreement implied that David would withhold nothing from the agents, including the contents of his memo book. But David's attempt to prevent Peterson from seeing the password, and his deletion of the heroin price list and attempted deletion of the firearms price list, clearly reflect that at the very least David did not *want* to share all of the contents of the book with the agents.

. . .

The critical question is whether David otherwise *impliedly* consented to the search of the contents of his book. To the extent that the book is analogous to a closed container, the agents' knowledge of the password is analogous to their possession of a key to the container. But unless the owner of the container voluntarily surrenders the key to the agents, their act of finding the key does not, in itself, give them the right to use it. Likewise, merely because Agent Peterson was able to see the password which could be used to "unlock" the book does not, without more, give him the right to use it. Moreover, David's failure to protest Peterson's use of the password is not equivalent to giving his approval of it." . . .

. . .

. . . Accordingly, the government should not be allowed to use as evidence the information which Agent Peterson obtained from the book when he accessed it without David's express consent.

The *third* event which had Fourth Amendment implications occurred when Agent Peterson grabbed the book out of David's hands after David deleted the heroin price list. This was unquestionably a seizure, because David has thereafter been deprived of the book.

The government argues that exigent circumstances justified the seizure. The Court agrees. When destruction of evidence is imminent, a warrantless seizure of that evidence is justified if

there is probable cause to believe that the item seized constitutes evidence of criminal activity. Here, Agent Peterson saw David destroying evidence. David's use of the book in retrieving telephone numbers of criminal associates provided ample probable cause that the book contained information relative to criminal activity. Peterson therefore reasonably believed that prompt action was necessary to prevent further destruction of relevant evidence.

The *fourth* and final event carrying Fourth Amendment implications was Peterson's act of reaccessing the book after its exigent seizure. Since that time Peterson has reviewed all of the contents of the book at his leisure. Clearly this qualifies as a search for Fourth Amendment purposes.

Although Peterson had the authority to seize and hold the book due to the exigency at hand, his authority to examine its contents is a different matter. The seizure of the book affected only David's possessory interests. It did not affect the privacy interests vested in the contents of the book.

The difference between possessory interests and privacy interests may justify a warrantless seizure of a container for the time necessary to secure a warrant, where a warrantless search of the contents would not be permissible. Peterson had ample probable cause to believe that the book contained information relating to criminal activity. Once he took the book from David the exigency which justified the seizure came to an end.[1] Nevertheless, without seeking a warrant, Peterson conducted a complete search of the book's contents. The seizure of the book did not justify the invasion of privacy involved in the subsequent search. Agent Peterson had ample time to obtain a search warrant, but failed to do so. His good faith belief that a warrant was unnecessary cannot save the illegality of the search. Therefore, the information which the government obtained from the book after the seizure, and any evidence derived from that information, must be suppressed at trial.

Coffeeshop problem

This problem is very loosely based on *In re Grand Jury Subpoena to Boucher*, No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007), *rev'd* 2009 WL 424718 (Feb. 19, 2009). Officer Augusta Zenobia from the King County Sheriff's Office is ordering an Americano at a Tully's Coffee Shop in Seattle when she notices that one of the other patrons has left an unattended laptop sitting on a table. It has shifted over into the screensaver, which appears to be pulling random pictures from the computer's hard drive. Some of them show people who appear to be . . . naked . . . and also . . . young.

A few seconds later, a man emerges from the men's room and walks towards the table with the laptop. He makes brief eye contact with Officer Zenobia, then looks back to the laptop, which has just flashed up another photo of someone without clothes on. He runs for the computer and slams it shut. Officer Zenobia is a few steps behind; she orders him away from the

[1] The government argues, lamely, that the exigency continued even after the seizure, because Agent Peterson did not know how much longer the book's batteries would live. It was therefore imperative, according to the government, that Peterson access the book before the batteries died and the information was erased. At the evidentiary hearing, however, no evidence was offered to substantiate this concern. In fact, Peterson testified that he successfully accessed the book at a later time without changing the batteries. The government bears a heavy burden of establishing exigent circumstances. Speculation is insufficient to carry that burden. The government has not met its burden here.

computer and places him under arrest. He turns out to be one Lucius Aurelian; he has a clean criminal record.

You work in the King County Prosecuting Attorney's office, and you have been assigned the case. Officer Zenobia is willing to testify that the images she saw were clearly child pornography. The lab technicians have reported that the computer's hard drive is encrypted. Without the password, they won't be able to recover any of the data on the hard drive.

You would like, if possible, to bring charges against Aurelian for the possession of child pornography. Your supervisor, who graduated from law school long before there was any such thing as "Internet Law," has suggested three possible ways to proceed:

1. Seek a court order requiring Aurelian to divulge the password.

2. Ask the lab technicians to try random words and short phrases as passwords (they have a computer program to automate the process) in the hopes that one of them will decrypt the hard drive.

3. Put the computer aside, focus on other aspects of the investigation, and rely solely on Officer Zenobia's testimony if necessary.

What should you do?

Zipper problem

This problem is very loosely based on real events. For more on them, see Steven Levy's book *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*.

Senator Bernard Abbott (R-TX) has become concerned about the balance of power in the cryptography world. It's afraid that criminals, terrorists, and foreign powers can too easily spy on Americans' communications—but that they're also using encryption to keep their own nefarious plans hidden. Accordingly, he's preparing legislation to standardized American cryptography. His bill would:

1. Require all telephones (land-line and cellular) and Internet connections in the United States to be built with a new, standard encryption technology called Zipper. Devices using Zipper would have unique ID numbers; whenever two Zipper devices established a connection, they'd use their unique IDs to negotiate a secret key to encrypt their communications. The two Zipper devices would be able to turn the encrypted message back into intelligible sounds, images, text or whatever, but anyone eavesdropping on the connection would see only random 1s and 0s.[1]

2. Well, *almost* anyone. The United States government would retain a "key escrow database" that contained a second secret key for each unique Zipper ID number. Zipper would be designed in such a way that the government could use the second secret key could *also* decrypt the communications. This database would be kept secure; a court order would be needed to allow law enforcement to look up the secret key for any given Zipper device.

---

[1] Yes, this actually works! The basic idea is a technique by the name of "Diffie-Hellman key exchange"; the math behind it is simple but a little mind-blowing. This technique is also one of the reasons why mathematicians have such a practical interest in prime numbers, as prime numbers form critical parts of the key.

3. In order to keep the system from breaking down, it would also be necessary to restrict the use of non-Zipper cryptography. Accordingly, after the implementation of Zipper, it would be illegal to encrypt communications using any other method.

4. Finally, to make sure that the U.S. has a sufficient lead in cryptography research, the Commerce Department will define encryption software as a "munition" and prohibit exporting it or making it available to foreign nationals.

You are on the legal staff of SETEC, a non-profit advocacy group that tries to keep the Internet open, free, and safe. You have just learned about Senator Abbott's proposal. You are flying to Washington for a meeting with the Senator's staff tomorrow. How will you try to talk them out of it? What arguments will they make, and how will you reply?

CLASS 15: WIRETAPPING

Today, we turn from information on a computer to information on the network. Our subject today is the *interception* of communications in transit from sender to recipient, or which are held by a third party. Our primary focus will be on statutory protections, but we'll also ask whether the two federal statutes on point—the Stored Communications Act (the SCA, codified at 18 U.S.C. §§ 2701 to 2712) and the Wiretap Act (codified at 18 U.S.C. §§ 2510 to 2522)—are constitutional. As we proceed, keep in mind two key distinctions:

- Are the communications being acquired by a private party or by the government?
- Are the communications being intercepted while in transit ("prospectively"), or retrieved after the fact ("retrospectively")?

Preparation questions

(1) Back to the statute books! (In case you haven't realized already, this is actually a legal skills course disguised as a doctrinal course. Today's subject: statute reading.) We start with the SCA. We've already met the provisions that govern access to subscriber information. Now we're ready to look at the provisions that govern access to stored communications themselves. Look at 18 U.S.C. § 2701(a) and § 2702(a)(1). What's the core behavior they're designed to prevent? What's the difference between them? Do these sections prohibit actions by private parties, by the government, or by both? And do these sections make Gmail illegal? After all, doesn't it "access" stored emails all the time? (Hint: read the rest of §§ 2701 and 2702.)

(2) The SCA's strong protection for stored communications is subject to a great many exceptions. Read the exceptions in sections 2701(c) and 2702(b). Which situations do they apply to? For whose benefit were they drafted? Which ones do you think are the most important and most frequently used in practice?

(3) The SCA also comes equipped with provision that allow the police to require the disclosure of stored communications under certain circumstances. Step one: Find the provision. Step two: identify the required showing the police must make. You should have discovered that the required showing depends on whether the communications have been in storage for less than 180 days or more than 180 days. Under what circumstances can the government gain access to stored electronic communications with less than a full search warrant? Can private parties avail themselves of this required disclosure procedure? What about the government acting in a non-law-enforcement capacity?

(4) The *Warshak* case raises the question of whether this statutory procedure is consistent with the Fourth Amendment. What does that mean, exactly? Go back to the Fourth Amendment issues discussed last time. What's the argument for why your emails on a New York Law School server should be subject to a different level of protection than your emails stored on your own computer? What's the argument that the level of protection should be the same? Which do you find more convincing? (The judgment of the panel that wrote the opinion reproduced below was vacated on ripeness grounds by the full Sixth Circuit, and the issue remains controversial.)

(5) Now, let's switch over to wiretapping. Look at § 2511, in conjunction with the relevant definitions in § 2510. What does the Wiretap Act prohibit? May I bug your telephone? Your

Skype? Your email? Wait a minute—what does it mean to "bug" your email? It seems pretty obvious what "intercept" means for wire or oral communications, right? But what does it mean for textual electronic communications transmitted in packets? Referring back to the Wiretap Act's definitions—which are essentially the same as the ones in the Florida statute—read *O'Brien* and ask whether its analysis of the meaning of "intercept" makes sense. Now that we've questioned the meaning of the term in the context of textual communications, take a step back and ask whether it's really so obvious what it means to "intercept" a Skype conversation? Try to think of hypotheticals about "interception" on a computer that push in both directions.

(6) Like the SCA, the Wiretap Act couples a strong—indeed criminal—prohibition to a set of exceptions. Compare the scope of the exceptions to the Wiretap Act (where?) to the exceptions to the SCA you analyzed above. Which are broader? Why? Now look at § 2518, which outlines the procedure for the police to install a wiretap. Is this harder or easier for them than it would be to acquire a search warrant? Can private parties obtain judicial authorization for one?

(7) Make a chart illustrating the Wiretap Act and the SCA. Try to fill in the different standards you've studied for today. Can you also fill in the provisions of the SCA that we studied in the class on anonymity?

Warshak v. United States
490 F.3d 455 (6th Cir. 2007), *vacated on other grounds*, 532 F.3d 521 (6th Cir. 2008) (en banc)

BOYCE F. MARTIN, JR., Circuit Judge.

. . . In March 2005, the United States was engaged in a criminal investigation of Plaintiff Steven Warshak and the company he owned, Berkeley Premium Nutraceuticals, Inc. The investigation pertained to allegations of mail and wire fraud, money laundering, and related federal offenses. On May 6, 2005, the government obtained an order from a United States Magistrate Judge in the Southern District of Ohio directing internet service provider ("ISP") NuVox Communications to turn over to government agents information pertaining to Warshak's e-mail account with NuVox. The information to be disclosed included (1) customer account information, such as application information, "account identifiers," "[b]illing information to include bank account numbers," contact information, and "[any] other information pertaining to the customer, including set up, synchronization, etc."; (2) "[t]he contents of wire or electronic communications (not in electronic storage unless greater than 181 days old) that were placed or stored in directories or files owned or controlled" by Warshak; and (3) "[a]ll Log files and backup tapes."

The order stated that it was issued under 18 U.S.C. § 2703, part of the Stored Communications Act ("SCA"), and that it was based on "specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought are relevant and material to an ongoing criminal investigation." The order was issued under seal, and prohibited NuVox from "disclos[ing] the existence of the Application or this Order of the Court, or the existence of this investigation, to the listed customer or to any person unless and until

authorized to do so by the Court." The magistrate further Ordered that "the notification by the government otherwise required under 18 U.S.C. § 2703(b)(1)(B) be delayed for ninety days." On September 12, 2005, the government obtained a nearly identical order pertaining to Yahoo, another ISP, that sought the same types of information from Warshak's Yahoo e-mail account and a Yahoo account identified with another individual named Ron Fricke.

On May 31, 2006, over a year after obtaining the NuVox order, the United States wrote to Warshak to notify him of both orders and their requirements. The magistrate had unsealed both orders the previous day. Based on this disclosure, Warshak filed suit on June 12, 2006, seeking declaratory and injunctive relief, and alleging that the compelled disclosure of his e-mails without a warrant violated the Fourth Amendment and the SCA. . . .

II.

The SCA, passed by Congress in 1986, is codified at 18 U.S.C. §§ 2701 to 2712, and contains a number of provisions pertaining to the accessibility of "stored wire and electronic communications and transactional records." Portions of the SCA that are not directly at stake here prohibit unauthorized access of electronic communications (§ 2701) and prohibit a service provider from divulging the contents of electronic communications that it is storing for a customer with certain exceptions pertaining to law enforcement needs (§ 2702). At issue in this case is § 2703, which provides procedures through which a governmental entity can access both user records and other subscriber information, and the content of electronic messages.

Subsection (a) requires the use of a warrant to access messages that have been in storage for 180 days or less. Subsection (b) provides that to obtain messages that have been stored for over 180 days, the government generally must either (1) obtain a search warrant, (2) use an administrative subpoena, or (3) obtain a court order. . . .

Subsection (d), which is referenced in subsection (b), sets forth the procedure and requirements for obtaining a court order (as opposed to a warrant):

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C. § 2703(d). The parties agree that the standard of proof for a court order —"specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . or records . . . are relevant and material to an ongoing criminal investigation"—falls short of probable cause. . . .

III.

B. Likelihood of Success on the Merits: Probable Cause versus Reasonableness and Fourth Amendment Implications of SCA Orders

. . .

Two amici curiae convincingly analogize the privacy interest that e-mail users hold in the content of their e-mails to the privacy interest in the content of telephone calls, recognized by the Supreme Court in its line of cases involving government eavesdropping on telephone conversations. *See Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); *Berger v. New York*, 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967). In *Berger* and *Katz*, telephone surveillance that intercepted the content of a conversation was held to constitute a search, because the caller "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," and therefore cannot be said to have forfeited his privacy right in the conversation. *Katz*, 389 U.S. at 352, 88 S.Ct. 507. This is so even though "[t]he telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment." *Smith*, 442 U.S. at 746, 99 S.Ct. 2577 (Stewart, J., dissenting). On the other hand, in *Smith*, the Court ruled that the use of pen register, installed at the phone company's facility to record the numbers dialed by the telephone user, did not amount to a search. This distinction was due to the fact that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the contents of communications." 442 U.S. at 741, 99 S.Ct. 2577 (emphasis in original).

The distinction between *Katz* and *Miller* makes clear that the reasonable expectation of privacy inquiry in the context of shared communications must necessarily focus on two narrower questions than the general fact that the communication was shared with another. First, we must specifically identify the party with whom the communication is shared, as well as the parties from whom disclosure is shielded. Clearly, under *Katz*, the mere fact that a communication is shared with another person does not entirely erode all expectations of privacy, because otherwise eaves dropping would never amount to a search. It is true, however, that by sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person, or obtained through a subpoena directed to that person. *See Miller*, 425 U.S. at 443, 96 S.Ct. 1619 ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."). The same does not necessarily apply, however, to an intermediary that merely has the ability to access the information sought by the government. Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service's ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them.

The second necessary inquiry pertains to the precise information actually conveyed to the party through whom disclosure is sought or obtained. This distinction provides the obvious crux for the different results in *Katz* and *Smith*, because although the conduct of the telephone user in Smith "may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.". Like the depositor in *Miller*, the caller in *Smith* "assumed the risk" of the

phone company disclosing the records that he conveyed to it. *Id.* Yet this assumption of the risk is limited to the specific information conveyed to the service provider, which in the telephone context excludes the content of the conversation. It is apparent, therefore, that although the government can compel disclosure of a shared communication from the party with whom it was shared, it can only compel disclosure of the specific information to which the subject of its compulsion has been granted access. It cannot, on the other hand, bootstrap an intermediary's limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation).

This focus on the specific information shared with the subject of compelled disclosure applies with equal force in the e-mail context. Compelled disclosure of subscriber information and related records through the ISP might not undermine the e-mail subscriber's Fourth Amendment interest under Smith, because like the information obtained through the pen register in Smith and like the bank records in Miller, subscriber information and related records are records of the service provider as well, and may likely be accessed by ISP employees in the normal course of their employment. Consequently, the user does not maintain the same expectation of privacy in them vis-a-vis the service provider, and a third party subpoena to the service provider to access information that is shared with it likely creates no Fourth Amendment problems. The combined precedents of *Katz* and *Smith*, however, recognize a heightened protection for the content of the communications. Like telephone conversations, simply because the phone company or the ISP **could** access the content of e-mails and phone calls, the privacy expectation in the **content** of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.

Similarly, under both *Miller* and *Katz*, if the government in this case had received the content of Warshak's e-mails by subpoenaing the person with whom Warshak was e-mailing, a Fourth Amendment challenge brought by Warshak would fail, because he would not have maintained a reasonable expectation of privacy vis-a-vis his e-mailing partners. *See Phibbs*, 999 F.2d at 1077. But this rationale is inapplicable where the party subpoenaed is not expected to access the content of the documents, much like the phone company in *Katz*. Thus, as Warshak argues, the government could not get around the privacy interest attached to a private letter by simply subpoenaing the postal service with no showing of probable cause, because unlike in *Phibbs*, postal workers would not be expected to read the letter in the normal course of business. *See Ex Parte Jackson*, 96 U.S. 727, 733, 24 L.Ed. 877 (1878) ("No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution."). Similarly, a bank customer maintains an expectation of privacy in a safe deposit box to which the bank lacks access (as opposed to bank records, like checks or account statements) and the government could not compel disclosure of the contents of the safe deposit box only by subpoenaing the bank.

This analysis is consistent with other decisions that have addressed an individual's expectation of privacy in particular electronic communications. In *Guest v. Leis*, 255 F.3d 325, 333 (6th Cir.2001), we concluded that users of electronic bulletin boards lacked an

expectation of privacy in material posted on the bulletin board, as such materials were "intended for publication or public posting." Of course the public disclosure of material to an untold number of readers distinguishes bulletin board postings from e-mails, which typically have a limited, select number of recipients. *See also Jackson*, 96 U.S. at 733 ("[A] distinction is to be made between different kinds of mail matter,—between what is intended to be kept free from inspection, such as letters, and sealed packages subject to letter postage; and what is open to inspection, such as newspapers, magazines, pamphlets, and other printed matter, purposely left in a condition to be examined."). Although we stated that an e-mail sender would "lose a legitimate expectation of privacy in an e-mail that had already reached its recipient," analogizing such an e-mailer to "a letter-writer," this diminished privacy is only relevant with respect to the recipient, as the sender has assumed the risk of disclosure by or through the recipient. *Id.* at 333 (citing *United States v. King*, 55 F.3d 1193, 1196 (6th Cir.1995)). *Guest* did not hold that the mere use of an intermediary such as an ISP to send and receive e-mails amounted to a waiver of a legitimate expectation of privacy.

Other courts have addressed analogous situations where electronic communications were obtained based on the sender's use of a computer network. In *United States v. Simons*, the Fourth Circuit held that a government employee lacked a reasonable expectation of privacy in electronic files on his office computer, in light of the employer's policy that explicitly notified the employee of its intention to "audit, inspect, and monitor," his computer files. 206 F.3d 392, 398 (4th Cir.2000). In light of this explicit policy, the employee's belief that his files were private was not objectively reasonable. Id. On the other hand, in United States v. Heckenkamp, the Ninth Circuit held that a university student did have a reasonable expectation of privacy in his computer files even though he "attached [his computer] to the university network," because the "university policies do not eliminate Heckenkamp's expectation of privacy in his computer." 482 F.3d 1142, 1147 (9th Cir.2007). Although the university did "establish limited instances in which university administrators may access his computer in order to protect the university's systems," this exception fell far short of a blanket monitoring or auditing policy, and the Ninth Circuit deemed it insufficient to waive the user's expectation of privacy.

Heckenkamp and *Simons* provide useful bookends for the question before us, regarding when the use of some intermediary provider of computer and e-mail services—be it a commercial ISP, a university, an employer, or another type of entity—amounts to a waiver of the user's reasonable expectation of privacy in the content of the e-mails with respect to that intermediary. In instances where a user agreement explicitly provides that e-mails and other files will be monitored or audited as in *Simons*, the user's knowledge of this fact may well extinguish his reasonable expectation of privacy. Without such a statement, however, the service provider's control over the files and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy, as in *Heckenkamp*.

Turning to the instant case, we have little difficulty agreeing with the district court that individuals maintain a reasonable expectation of privacy in e-mails that are stored with, or sent or received through, a commercial ISP. The content of e-mail is something that the user "seeks to preserve as private," and therefore "may be constitutionally protected." *Katz*, 389 U.S. at 351, 88 S.Ct. 507. It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today

as protecting telephone conversations has been in the past. *See Katz*, 389 U.S. at 352, 88 S.Ct. 507 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.")

The government asserts that ISPs have the contractual right to access users' e-mails. The district court's ruling was based on its willingness to credit Warshak's contrary factual argument that "employees of commercial ISPs [do not] open and read—[nor do] their subscribers reasonably expect them to open and read— individual subscriber e-mails as a matter of course." This factual determination tracks the language from *Miller* and *Phibbs* that suggests a privacy interest in records held by a third party is only undermined where the documents are accessed by the third party or its employees "in the ordinary course of business." *Miller*, 425 U.S. at 442, 96 S.Ct. 1619. Moreover, as explained in the Ninth Circuit's decision in *Heckenkamp*, mere accessibility is not enough to waive an expectation of privacy. *See Heckenkamp*, 482 F.3d at 1147 (holding that university policies establishing "limited instances in which university administrators may access [the user's] computer in order to protect the university's systems" was insufficient to eliminate an expectation of privacy); *see also Katz*, 389 U.S. at 351, 88 S.Ct. 507 ("[W]hat [a pay phone user] seeks to preserve as private, **even in an area accessible to the public,** may be constitutionally protected." (emphasis added)). Where a user agreement calls for regular auditing, inspection, or monitoring of e-mails, the expectation may well be different, as the potential for an administrator to read the content of e-mails in the account should be apparent to the user. *See Simons*, 206 F.3d at 398. Where there is such an arrangement, compelled disclosure by means of an SCA order directed at the ISP would be akin to the third party subpoena directed at a bank, as in *Miller* and *Jerry T. O'Brien*. In contrast, the terms of service in question here, which the government has cited to in both the district court and this Court, clearly provide for access only in limited circumstances, rather than wholesale inspection, auditing, or monitoring of e-mails. Because the ISPs right to access e-mails under these user agreements is reserved for extraordinary circumstances, much like the university policy in *Heckenkamp*, it is similarly insufficient to undermine a user's expectation of privacy. For now, the government has made no showing that e-mail content is regularly accessed by ISPs, or that users are aware of such access of content.

The government also insists that ISPs regularly screen users' e-mails for viruses, spam, and child pornography. Even assuming that this is true, however, such a process does not waive an expectation of privacy in the content of e-mails sent through the ISP, for the same reasons that the terms of service are insufficient to waive privacy expectations. The government states that ISPs "are developing technology that will enable them to scan user images" for child pornography and viruses. The government's statement that this process involves "technology," rather than manual, human review, suggests that it involves a computer searching for particular terms, types of images, or similar indicia of wrongdoing that would not disclose the content of the e-mail to any person at the ISP or elsewhere, aside from the recipient. But the reasonable expectation of privacy of an e-mail user goes to the **content** of the e-mail message. The fact that a computer scans millions of e-mails for signs of pornography or a virus does not invade an individual's content-based privacy interest in the e-mails and has little bearing on his expectation of privacy in the content. In fact, these screening processes are analogous to the post office screening packages for evidence of drugs or explosives, which does not expose the content of written documents enclosed in the

packages. The fact that such screening occurs as a general matter does not diminish the well-established reasonable expectation of privacy that users of the mail maintain in the packages they send.

It is also worth noting that other portions of the SCA itself strongly support an e-mail user's reasonable expectation of privacy in the content of his e-mails. Section 2701 prohibits unauthorized users from accessing e-mails. Section 2702 generally prohibits an ISP from disclosing e-mail content without the permission of the user. Further, section 2703 makes it easier for the government to get an order requiring the disclosure of records and subscriber information, in which the user does not maintain a privacy interest vis-a-vis the ISP, than to obtain an order requiring the disclosure of content. The statute also requires a warrant to search the content of e-mails that have been stored for 180 days or less. 18 U.S.C. 1703(a). Thus, even though the contested exception in section 2703(b) creates tension with the Fourth Amendment's requirements for a warrant, independent provisions support the proposition that a user maintains a reasonable expectation of privacy in the content of his e-mails. . . .

O'Brien v. O'Brien
899 So. 2d 1133 (Fla. Dist. Ct. App.-5th 2005)

SAWAYA, C.J.

Emanating from a rather contentious divorce proceeding is an issue we must resolve regarding application of certain provisions of the Security of Communications Act (the Act) found in Chapter 934, Florida Statutes (2003). Specifically, we must determine whether the trial court properly concluded that pursuant to section 934.03(1), Florida Statutes (2003), certain communications were inadmissible because they were illegally intercepted by the Wife who, unbeknownst to the Husband, had installed a spyware program on a computer used by the Husband that copied and stored electronic communications between the Husband and another woman.

When marital discord erupted between the Husband and the Wife, the Wife secretly installed a spyware program called Spector on the Husband's computer. It is undisputed that the Husband engaged in private on-line chats with another woman while playing Yahoo Dominoes on his computer. The Spector spyware secretly took snapshots of what appeared on the computer screen, and the frequency of these snapshots allowed Spector to capture and record all chat conversations, instant messages, e-mails sent and received, and the websites visited by the user of the computer. When the Husband discovered the Wife's clandestine attempt to monitor and record his conversations with his Dominoes partner, the Husband uninstalled the Spector software and filed a Motion for Temporary Injunction, which was subsequently granted, to prevent the Wife from disclosing the communications. . . .

. . . The Wife argues that the electronic communications do not fall under the umbra of the Act because these communications were retrieved from storage and, therefore, are not "intercepted communications" as defined by the Act. In opposition, the Husband contends that the Spector spyware installed on the computer acquired his electronic communications real-time as they were in transmission and, therefore, are intercepts illegally obtained under the Act.

The trial court found that the electronic communications were illegally obtained in violation of section 934.03(1)(a)(e), and so we begin our analysis with the pertinent provisions of that statute, which subjects any person to criminal penalties who engages in the following activities:

> (a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication; . . .

§ 934.03(1)(a)-(e), Fla. Stat. (2003).

. . . It is beyond doubt that what the trial court excluded from evidence are "electronic communications." The core of the issue lies in whether the electronic communications were intercepted. The term "intercept" is defined by the Act 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." § 934.02(3), Fla. Stat. (2003). We discern that there is a rather fine distinction between what is transmitted as an electronic communication subject to interception and the storage of what has been previously communicated. It is here that we tread upon new ground. Because we have found no precedent rendered by the Florida courts that considers this distinction, and in light of the fact that the Act was modeled after the Federal Wiretap Act, we advert to decisions by the federal courts that have addressed this issue for guidance

The federal courts have consistently held that electronic communications, in order to be intercepted, must be acquired contemporaneously with transmission and that electronic communications are not intercepted within the meaning of the Federal Wiretap Act if they are retrieved from storage. . . . [T]he particular facts and circumstances of the instant case reveal that the electronic communications were intercepted contemporaneously with transmission.

The Spector spyware program that the Wife surreptitiously installed on the computer used by the Husband intercepted and copied the electronic communications as they were transmitted. We believe that particular method constitutes interception within the meaning of the Florida Act, and the decision in *Steiger* supports this conclusion. In *Steiger*, an individual was able to hack into the defendant's computer via a Trojan horse virus that allowed the hacker access to pornographic materials stored on the hard drive. The hacker was successful in transferring the pornographic material from that computer to the hacker's computer. The court held that because the Trojan horse virus simply copied information that had previously been stored on the computer's hard drive, the capture of the electronic communication was not an interception within the meaning of the Federal Wiretap Act. The court did indicate, however, that interception could occur if the virus or software intercepted the communication as it was being transmitted and copied it. The court stated:

> [T]here is only a narrow window during which an E-mail interception may occur—the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.

Steiger, 318 F.3d at 1050 (quoting Jarrod J. White, *E-Mail@Work.com: Employer Monitoring of Employee E-Mail*, 48 Ala. L.Rev. 1079, 1083 (1997)). Hence, a valid distinction exists between a spyware program similar to that in *Steiger*, which simply breaks into a computer and retrieves information already stored on the hard drive, and a spyware program similar to the one installed

by the Wife in the instant case, which copies the communication as it is transmitted and routes the copy to a storage file in the computer.

The Wife argues that the communications were in fact stored before acquisition because once the text image became visible on the screen, the communication was no longer in transit and, therefore, not subject to intercept. We disagree. We do not believe that this evanescent time period is sufficient to transform acquisition of the communications from a contemporaneous interception to retrieval from electronic storage. We conclude that because the spyware installed by the Wife intercepted the electronic communication contemporaneously with transmission, copied it, and routed the copy to a file in the computer's hard drive, the electronic communications were intercepted in violation of the Florida Act.

. . .

CLASS 16: PRIVACY

Our final topic in the privacy unit is the personal privacy issues that arise out of ordinary web use. What do web sites know about you, what can they do with that information, and what information do you expose about yourself to the world?

Preparation questions

(1) We start with cookies. They were originally designed to allow users to log in to web sites and have the sites remember them later. The web site "sets a cookie" when you log in; later, it "retrieves" the cookie and recognizes you. Companies like DoubleClick figured out how to use this technology to serve personalized ads. The court's discussion of how cookies work is a bit dry. Can you do better? (Outside research is fine. It's often the best approach when you run across something slightly mysterious in terms of how the Internet works.) Draw a picture; what information is transmitted to whom, and when?

(2) The *DoubleClick* case holds that DoubleClick's use of cookies violates neither the SCA nor the Wiretap Act. Why? Are you convinced by the court's reading of the statutes? Once you draw the pictures, do cookies seem more or less like a form of worrisome surveillance? Is the harm here a harm of the sort these laws were intended to prevent?

(3) Or is it not a harm at all? DoubleClick has always described itself as offering consumers (*not* just advertisers) a highly useful service. What service is that? How useful do you find it? How would the Web change if DoubleClick-style tracking cookies were banned tomorrow? What would be the impact on web sites and advertisers? Which forms of web advertising do you find most annoying? Creepiest? Which, if any, would you prohibit?

(4) DoubleClick offers an opt-out from its cookie tracking at http://www.doubleclick.com/privacy/dart_adserving.aspx. The fraction of Internet users who've opted out it is infinitesimal. Why might that be? Does the fact that most users haven't opted out indicate that they don't care about personal privacy of this sort? The FTC is considering imposing an opt-in system instead. What's the difference? Would such a rule be a good idea?

(5) Our second big topic is privacy policies. One recent survey found that six out of ten Americans surveyed responded "true" to the question, "If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission." Now that you've read *JetBlue*, are they correct? Does their belief have any implications for privacy law and policy? Could it potentially change the analysis in *JetBlue* itself? After reading the case, are you inclined to change your online behavior in any significant respects?

(6) Finally, we'll talk about social networks and privacy. I've given you a few stories from Chris Petersen's paper on Facebook and privacy. Do they ring true with your experience? Do you have other stories about privacy failures or successes on social network sites? Is Facebook good or bad for privacy? What, if anything, can and should the law do about it? Is the Internet killing privacy? Do "the kids today" no longer care about privacy? What is privacy, what if anything is it good for, and what's its future in the Internet age?

BUCHWALD, District Judge.

Plaintiffs bring this class action on behalf of themselves and all others similarly situatedagainst defendant DoubleClick, Inc. ("defendant" or "DoubleClick") seeking injunctive and monetary relief for injuries they have suffered as a result of DoubleClick's purported illegal conduct. . . .

PROCEDURAL HISTORY

This case is a multidistrict consolidated class action. The initial complaint was filed in this Court on January 31, 2000. On May 10, 2000, this Court consolidated the set of related federal class actions against DoubleClick in the Southern and Eastern Districts of New York pursuant to Rule 42(a) of the Fed.R.Civ.P. and Local Rule 1.6 of the Southern and Eastern Districts of New York. . . .

BACKGROUND

DoubleClick, a Delaware corporation, is the largest provider of Internet advertising products and services in the world. Its Internet-based advertising network of over 11,000 Web publishers has enabled DoubleClick to become the market leader in delivering online advertising. DoubleClick specializes in collecting, compiling and analyzing information about Internet users through proprietary technologies and techniques, and using it to target online advertising. DoubleClick has placed billions of advertisements on its clients' behalf and its services reach the majority of Internet users in the United States. . . .

DOUBLECLICK'S TECHNOLOGY AND SERVICES

DoubleClick provides the Internet's largest advertising service. Commercial Web sites often rent-out online advertising "space" to other Web sites. In the simplest type of arrangement, the host Web site (e.g., Lycos.com) rents space on its webpages to another Web site (e.g., The-Globe.com) to place a "hotlink" banner advertisement ("banner advertisement"). When a user on the host Web site "clicks" on the banner advertisement, he is automatically connected to the advertiser's designated Web site.

DoubleClick acts as an intermediary between host Web sites and Web sites seeking to place banner advertisements. It promises client Web sites that it will place their banner advertisements in front of viewers who match their demographic target. For example, DoubleClick might try to place banner advertisements for a Web site that sells golfclubs in front of high-income people who follow golf and have a track record of making expensive online purchases. DoubleClick creates value for its customers in large part by building detailed profiles of Internet users and using them to target clients' advertisements. . . .

When users visit any of these DoubleClick-affiliated Web sites, a "cookie" is placed on their hard drives. Cookies are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner. However, Plaintiffs allege that DoubleClick's cookies collect "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.". DoubleClick's cookies store this personal information on users' hard drives until DoubleClick electronically accesses the cookies and uploads the data.

How DoubleClick targets banner advertisements and utilizes cookies to collect user information is crucial to our analysis under the three statutes. Therefore, we examine both processes in greater detail.

A. Targeting Banner Advertisements

DoubleClick's advertising targeting process involves three participants and four steps. The three participants are: (1) the user; (2) the DoubleClick-affiliated Web site; (3) the DoubleClick server. For the purposes of this discussion, we assume that a DoubleClick cookie already sits on the user's computer with the identification number "# 0001."

In Step One, a user seeks to access a DoubleClick-affiliated Web site such as Lycos.com. The user's browser sends a communication to Lycos.com (technically, to Lycos.com's server) saying, in essence, "Send me your homepage." This communication may contain data submitted as part of the request, such as a query string or field information.

In Step Two, Lycos.com receives the request, processes it, and returns a communication to the user saying "Here is the Web page you requested." The communication has two parts. The first part is a copy of the Lycos.com homepage, essentially the collection article summaries, pictures and hotlinks a user sees on his screen when Lycos.com appears. The only objects missing are the banner advertisements; in their places lie blank spaces. The second part of the communication is an IP-address link to the DoubleClick server. This link instructs the user's computer to send a communication automatically to DoubleClick's server.

In Step Three, as per the IP-address instruction, the user's computer sends a communication to the DoubleClick server saying "I am cookie # 0001, send me banner advertisements to fill the blank spaces in the Lycos.com Web page." This communication contains information including the cookie identification number, the name of the DoubleClick-affiliated Web site the user requested, and the user's browsertype.

Finally, in Step Four, the DoubleClick server identifies the user's profile by the cookie identification number and runs a complex set of algorithms based, in part, on the user's profile, to determine which advertisements it will present to the user. It then sends a communication to the user with banner advertisements saying "Here are the targeted banner advertisements for the Lycos.com homepage." Meanwhile, it also updates the user's profile with the information from the request.

DoubleClick's targeted advertising process is invisible to the user. His experience consists simply of requesting the Lycos.com homepage and, several moments later, receiving it complete with banner advertisements.

B. Cookie Information Collection

DoubleClick's cookies only collect information from one step of the above process: Step One. The cookies capture certain parts of the communications that users send to DoubleClick-

affiliated Web sites. They collect this information in three ways: (1) "GET" submissions, (2) "POST" submissions, and (3) "GIF" submissions.

GET information is submitted as part of a Web site's address or "URL," in what is known as a "query string." For example, a request for a hypothetical online record store's selection of Bon Jovi albums might read: http://recordstore.hypothetical. com/search?terms=bonjovi. The URL query string begins with the "?" character meaning the cookie would record that the user requested information about Bon Jovi.

Users submit POST information when they fill-in multiple blank fields on a web-page. For example, if a user signed-up for an online discussion group, he might have to fill-in fields with his name, address, email address, phone number and discussion group alias. The cookie would capture this submitted POST information.

Finally, DoubleClick places GIF tags on its affiliated Web sites. GIF tags are the size of a single pixel and are invisible to users. Unseen, they record the users' movements throughout the affiliated Web site, enabling DoubleClick to learn what information the user sought and viewed.

Although the information collected by DoubleClick's cookies is allegedly voluminous and detailed, it is important to note three clearly defined parameters. First, DoubleClick's cookies only collect information concerning users' activities on DoubleClick-affiliated Web sites. Thus, if a user visits an unaffiliated Web site, the DoubleClick cookie captures no information. Second, plaintiff does not allege that DoubleClick ever attempted to collect any information other than the GET, POST, and GIF information submitted by users. DoubleClick is never alleged to have accessed files, programs or other information on users' hard drives. Third, DoubleClick will not collect information from any user who takes simple steps to prevent DoubleClick's tracking. As plaintiffs' counsel demonstrated at oral argument, users can easily and at no cost prevent DoubleClick from collecting information from them. They may do this in two ways: (1) visiting the DoubleClick Web site and requesting an "opt-out" cookie; and (2) configuring their browsers to block any cookies from being deposited.

Once DoubleClick collects information from the cookies on users' hard drives, it aggregates and compiles the information to build demographic profiles of users. Plaintiffs allege that DoubleClick has more than 100 million user profiles in its database. Exploiting its proprietary Dynamic Advertising Reporting & Targeting ("DART") technology, DoubleClick and its licenseestarget banner advertisements using these demographic profiles. . . .

DISCUSSION

. . .

Claim I. Title II of the ECPA

Title II ("Title II") of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §2701 et seq. ("§ 2701"), aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications. It creates both criminal sanctions and a civil right of actionagainst persons who gain unauthorized access to communications facilities and thereby access electronic communications stored incident to their transmission. Title II specifically defines the relevant prohibited conduct as follows:

> "(a) Offense. Except as provided in subsection (c) of this section whoever(1) intentionally accesses without authorization a facility through which an electronic

> information service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains ... access to a wire or electronic communication while it is in electronic storage in such system shall be punished...."

Plaintiffs contend that DoubleClick's placement of cookies on plaintiffs' hard drives constitutes unauthorized access and, as a result, DoubleClick's collection of information from the cookiesviolates Title II. However, Title II contains an exception to its general prohibition.

> "(c) Exceptions.-Subsection (a) of this section does not apply with respect to conduct authorized... (2) by a user of that [wire or electronic communications] service with respect to a communication of or intended for that user;"

DoubleClick argues that its conduct falls under this exception. It contends that the DoubleClick-affiliated Web sites are "users" of the Internet and that all of plaintiffs' communications accessed by DoubleClick's cookies have been "of or intended for" these Web sites. Therefore, it asserts, the Web sites' authorization excepts DoubleClick's access from § 2701 (a)'s general prohibition. . . .

Assuming that the communications are considered to be in "electronic storage," it appears that plaintiffs have adequately pled that DoubleClick's conduct constitutes an offense under § 2701(a), absent the exception under § 2701(c)(2). Therefore, the issue is whether DoubleClick's conduct falls under § 2701(c)(2)'s exception. This issue has three parts: (1) what is the relevant electronic communications service?; (2) were DoubleClick-affiliated Web sites "users" of this service?; and (3) did the DoubleClick-affiliated Web sites give DoubleClick sufficient authorization to access plaintiffs' stored communications "intended for" those Web sites?

A. "Internet Access" is the relevant electronic communications service.

Obviously, in a broad sense, the "Internet" is the relevant communications service.However, for the purposes of this motion, it is important that we define Internet service with somewhat greater care and precision. Plaintiff, at turns, argues that the electronic communications service is "Internet access" and "the ISP [Internet Service Provider]." The difference is important. An ISP is an entity that provides access to the Internet; examples include America Online, UUNET and Juno. Access to the Internet is the service an ISP provides. Therefore, the "service which provides to users thereof the ability to send or receive wire or electronic communications" is "Internet access."

B. Web Sites are "users" under the ECPA.

The ECPA defines a "user" as "any person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13). On first reading, the DoubleClick-affiliated Web sites appear to be users—they are (1) "entities" that (2) use Internet access and (3) are authorized to use Internet access by the ISPs to which they subscribe. However, plaintiffs make two arguments that Web sites nevertheless are not users. Both are unpersuasive. . . .

One final point bears mention, even though plaintiffs did not raise it. One could imagine a facially sensible argument that Web sites are not "users" of Internet access because they are passive storage receptacles for information; the human is the "user" and the Web site is what is used. However, the Internet's engineering belies this description. Because the Internet functions through packet-switching and dynamic routing, human users do not in any sense connect to a

passive receptacle and obtain information. Indeed, no direct connection ever exists between the human user and the Web site. Rather, the human user sends a request to which the Web site must actively respond: processing the request, deciding whether to provide the information sought, obtaining the document from the server, translating the document into TCP/IP protocol, sending the packets and awaiting confirmation of their arrival. Indeed, in a practical sense, Web sites are among the most active "users" of Internet access—their existence and utility depend on it, unlike humans. Therefore, we find as a matter of law that the DoubleClick-affiliated Web sites are "users" of Internet access under the ECPA.

C. All of the communications DoubleClick has accessed through its cookies have been authorized or have fallen outside of Title II's scope.

Because plaintiffs only allege that DoubleClick accessed communications from plaintiffs to DoubleClick-affiliated Web sites, the issue becomes whether the Web sites gave DoubleClick adequate authorization under § 2701(c)(2) to access those communications. This issue, in turn, has two parts: (1) have the DoubleClick-affiliated Web sites authorized DoubleClick to access plaintiffs' communications to them?; and (2) is that authorization sufficient under § 2701(c)(2)?

1. The DoubleClick-affiliated Web sites have consented to DoubleClick's interception of plaintiffs' communications. . . .

Examining DoubleClick's technological and commercial relationships with its affiliated Web sites, we find it implausible to infer that the Web sites have not authorized DoubleClick's access. In a practical sense, the very reason clients hire DoubleClick is to target advertisements based on users' demographic profiles. DoubleClick has trumpeted this fact in its advertising, patents and Securities and Exchange filings. True, officers of certain Web sites might not understand precisely how DoubleClick collects demographic information through cookies and records plaintiffs' travels across the Web. However, that knowledge is irrelevant to the authorization at issue—Title II in no way outlaws collecting personally identifiable information or placing cookies, qua such. All that the Web sites must authorize is that DoubleClick access plaintiffs' communications to them. As described in the earlier section "Targeting Banner Advertisements," the DoubleClick-affiliated Web sites actively notify DoubleClick each time a plaintiff sends them an electronic communication (whether through a page request, search, or GIF tag). The data in these notifications (such as the name of the Web site requested) often play an important role in determining which advertisements are presented to users. Plaintiffs have offered no explanation as to how, in anything other than a purely theoretical sense, the DoubleClick-affiliated Web sites could have played such a central role in the information collection and not have authorized DoubleClick's access. This purely theoretical possibility that a DoubleClick-affiliated Web site might have been so ignorant as to have been unaware of the defining characteristic of DoubleClick's advertising service—the service the Web site knowingly and purposely purchased—and its own role in facilitating that service, is too remote to be the basis for extensive and costly discovery of DoubleClick and its affiliates. Therefore, we find that the DoubleClick-affiliated Web sites consented to DoubleClick's access of plaintiffs' communications to them.

2. DoubleClick is authorized to access plaintiffs' GET, POST and GIF submissions to the DoubleClick-affiliated Web sites.

Plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all "intended for" those Web sites. In the case of the GET and POST submissions, users voluntarily

type-in information they wish to submit to the Web sites, information such as queries, commercial orders, and personal information. GIF information is generated and collected when users use their computer "mouse" or other instruments to navigate through Web pages and access information. Although the users' requests for data come through clicks, not keystrokes, they nonetheless are voluntary and purposeful. Therefore, because plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all "intended for" those Web sites, the Web sites' authorization is sufficient to except DoubleClick's access under § 2701(c)(2). . . .

3. To the extent that the DoubleClick cookies' identification numbers are electronic communications, (1) they fall outside of Title II's scope, and (2) DoubleClick's access to them is otherwise authorized. . . .

(b) If the DoubleClick cookies' identification numbers are considered stored electronic communications, they are "of or intended for" DoubleClick and DoubleClick's acquisition of them does not violate Title II.

Even if we were to assume that cookies and their identification numbers were "electronic communication[s] ... in electronic storage," DoubleClick's access is still authorized. Section 2701 (c)(2) excepts from Title II's prohibition access, authorized by a "user," to communications (1) "of" (2) "or intended for" that user. In every practical sense, the cookies' identification numbers are internal DoubleClick communications—"both "of" and "intended for" DoubleClick. DoubleClick creates the cookies, assigns them identification numbers, and places them on plaintiffs' hard drives. The cookies and their identification numbers are vital to DoubleClick and meaningless to anyone else. In contrast, virtually all plaintiffs are unaware that the cookies exist, that these cookies have identification numbers, that DoubleClick accesses these identification numbers and that these numbers are critical to DoubleClick's operations.

In this sense, cookie identification numbers are much akin to computer bar-codes or identification numbers placed on "business reply cards" found in magazines. These bar-codes and identification numbers are meaningless to consumers, but are valuable to companies in compiling data on consumer responses (e.g. from which magazine did the consumer get the card?). Although consumers fill-out business reply cards and return them to companies by mail, the bar-codes and identification numbers that appear on the cards are purely internal administrative data for the companies. The cookie identification numbers are every bit as internal to DoubleClick as the bar-codes and identification numbers are to business reply mailers. Therefore, it seems both sensible to consider the identification numbers to be "of or intended for" DoubleClick and bizarre to describe them as "of or intended for" plaintiffs. Accordingly, because the identification numbers are "of or intended for" DoubleClick, it does not violate Title II for DoubleClick to obtain them from plaintiffs' electronic storage.

To summarize, plaintiffs' GET, POST and GIF submissions are excepted from § 2701(c)(2) because they are "intended for" the DoubleClick-affiliated Web sites who have authorized DoubleClick's access. The cookie identification numbers sent to DoubleClick from plaintiffs' computers fall outside of Title II's protection because they are not in "electronic storage" and,even if they were, DoubleClick is authorized to access its own communications.

In light of the above findings, we rule that all of plaintiffs' communications accessed by DoubleClick fall under § 2701(c)(2)'s exception or outside Title II and, accordingly, are not actionable. Therefore, plaintiffs' claim under the Title II (Claim I) is dismissed.

Claim II. Wiretap Act

Plaintiffs' second claim is that DoubleClick violated the Federal Wiretap Act ("Wiretap Act"), 18 U.S.C. § 2510, et seq. The Wiretap Act provides for criminal punishment and a private right of action against:

> "any person who—"(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept wire, oral, or electronic communication [except as provided in the statute]." 18 U.S.C. § 2511.

For the purposes of this motion, DoubleClick concedes that its conduct, as pled, violates this prohibition. However, DoubleClick claims that its actions fall under an explicit statutory exception:

> "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or any State." 18 U.S.C. § 2511(2)(d) ("§ 2511(2)(d)") (emphasis added).

DoubleClick argues once again that the DoubleClick-affiliated Web sites have consented to its interceptions and, accordingly, that its conduct is exempted from the Wiretap Act's general prohibition as it was from the Title II's. Plaintiffs deny that the Web sites have consented and argue that even if the Web sites do consent, the exception does not apply because DoubleClick's purpose is to commit "criminal or tortious act[s]."

As a preliminary matter, we find that the DoubleClick-affiliated Web sites are "parties to the communication[s]" from plaintiffs and have given sufficient consent to DoubleClick to intercept them. In reviewing the case law and legislative histories of Title II and the Wiretap Act, we can find no difference in their definitions of "user" (Title II) and "parties to the communication" (Wiretap Act) or "authorize" (Title II) and "consent" (Wiretap Act) that would make our analysis of the Web sites' consent under Title II inapplicable to the Wiretap Act. *See* discussion *supra* Section I(C). . . .

To summarize, we find that the DoubleClick-affiliated Web sites are "parties" to plaintiffs' intercepted communications under the Wiretap Act and that they consent to DoubleClick's interceptions. . . .

In re JetBlue Airways Corp. Privacy Litig.
379 F. Supp. 2d 299 (E.D.N.Y. 2005)

AMON, District Judge.

INTRODUCTION

A nationwide class of plaintiffs brings this action against JetBlue Airways Corporation ("JetBlue"), Torch Concepts, Inc. ("Torch"), Acxiom Corporation ("Acxiom"), and SRS Technologies ("SRS") for alleged violations of the Electronic Communications Privacy Act of

1986 ("ECPA"), 18 U.S.C. § 2701, *et seq.* (1986), and violations of state and common law. Plaintiffs claim that defendants violated their privacy rights by unlawfully transferring their personal information to Torch for use in a federally-funded study on military base security. Plaintiffs seek a minimum of $1,000 in damages per class member, or injunctive relief to the extent that damages are unavailable, as well as a declaratory judgment. Defendants have moved to dismiss the Amended Complaint pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure on the grounds that plaintiffs have failed to state a federal cause of action under the ECPA, that plaintiffs' state law claims are federally preempted, and that plaintiffs have failed to state any claim under state law.

STATEMENT OF FACTS

Unless otherwise indicated, the following facts set forth in plaintiffs' Amended Complaint are presumed to be true for purposes of defendants' motions to dismiss. JetBlue has a practice of compiling and maintaining personal information, known in the airline industry as Passenger Name Records ("PNRs"), on each of its adult and minor passengers. Information contained in PNRs includes, for example, passenger names, addresses, phone numbers, and travel itineraries. The PNRs are maintained, or temporarily stored, on JetBlue's computer servers, and passengers are able to modify their stored information. Acxiom, a world leader in customer and information management solutions, maintains personally-identifiable information on almost eighty percent of the U.S. population, including many JetBlue passengers, which it uses to assist companies such as JetBlue in customer and information management solutions.

The personal information that forms the basis of JetBlue's PNRs is obtained from its passengers over the telephone and through its Internet website during the selection and purchase of travel arrangements. In order to encourage the provision of personal information in this manner, JetBlue created a privacy policy which provided that the company would use computer IP addresses only to help diagnose server problems, cookies to save consumers' names, e-mail addresses to alleviate consumers from having to re-enter such data on future occasions, and optional passenger contact information to send the user updates and offers from JetBlue. The JetBlue privacy policy specifically represented that any financial and personal information collected by JetBlue would not be shared with third parties and would be protected by secure servers. JetBlue also purported to have security measures in place to guard against the loss, misuse, or alteration of consumer information under its control.

In the wake of September 11, 2001, Torch, a data mining company similar to Acxiom, presented the Department of Defense ("DOD") with a data pattern analysis proposal geared toward improving the security of military installations in the United States and possibly abroad. Torch suggested that a rigorous analysis of personal characteristics of persons who sought access to military installations might be used to predict which individuals pose a risk to the security of those installations. DOD showed interest in Torch's proposal and added Torch as a subcontractor to an existing contract with SRS so that Torch could carry out a limited initial test of its proposed study. The SRS contract was amended to include airline PNRs as a possible data source in connection with Torch's study. Because Torch needed access to a large national-level database of personal information and because no federal agencies approached by Torch would grant access to their own governmental databases, Torch independently contacted a number of airlines in search of private databases that might contain adequate information to serve its requirements. These airlines declined to share their passengers' personal information unless the Department of

Transportation ("DOT") and/or the Transportation Security Administration ("TSA") were involved and approved of such data sharing.

Unable to obtain the data through its own devices, Torch asked members of Congress to intervene on its behalf with the airlines or federal agencies. Torch also contacted the DOT directly. Following a series of meetings, the DOT and the TSA agreed to assist Torch in obtaining consent from a national airline to share its passenger information. On July 30, 2002, the TSA sent JetBlue a written request to supply its data to the DOD, and JetBlue agreed to cooperate. In September 2002, JetBlue and Acxiom collectively transferred approximately five million electronically-stored PNRs to Torch in connection with the SRS/DOD contract. Then, in October 2002, Torch separately purchased additional data from Acxiom for use in connection with the SRS contract. This data was merged with the September 2002 data to create a single database of JetBluepassenger information including each passenger's name, address, gender, home ownership or rental status, economic status, social security number, occupation, and the number of adults and children in the passenger's family as well as the number of vehicles owned or leased. Using this data, Torch began its data analysis and created a customer profiling scheme designed to identify high-risk passengers among those traveling on JetBlue.

In or about September 2003, government disclosures and ensuing public investigations concerning the data transfer to Torch prompted JetBlue Chief Executive Officer David Neelman to acknowledge that the transfer had been a violation of JetBlue's privacy policy. A class of plaintiffs whose personal information was among that transferred now brings this action against JetBlue, Torch, Acxiom, and SRS, seeking monetary damages, including punitive damages, and injunctive relief. . . .

DISCUSSION

I. Legal Standard for Rule 12(b)(6) Motion to Dismiss

In deciding a motion to dismiss pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure for failure to state a claim upon which relief can be granted, a court must accept the factual allegations in the complaint as true and draw all reasonable inferences in favor of the plaintiff. *See Press v. Chemical Inv. Servs. Corp.*, 166 F.3d 529, 534 (2d Cir.1999). The Court need not accept general, conclusory allegations as true, however, when they are belied by more specific allegations in the complaint. *Hirsch v. Arthur Andersen & Co.*, 72 F.3d 1085, 1092 (2d Cir.1995). Dismissal is proper "only where it appears beyond doubt that the plaintiff can prove no set of facts in support of the claim which would entitle him to relief." *Scotto v. Almenas*, 143 F.3d 105, 109-10 (2d Cir.1998) (quoting *Branham v. Meachum*, 77 F.3d 626, 628 (2d Cir.1996)). With these standards in mind, the Court turns to analysis of the claims raised in plaintiffs' Amended Complaint.

II. Electronic Communications Privacy Act

[The Court dismissed the plaintiffs' claims under § 2702 of the Stored Communications Act. Why?]

V. Failure to State a Claim Under State or Common Law

A. Breach of Contract

JetBlue is the only defendant charged with breach of contract in this case. Plaintiffs allege that they made reservations to fly with JetBlue in reliance on express promises made by JetBlue in

the company's privacy policy. The substance of the contract alleged is therefore a promise by JetBlue not to disclose passengers' personal information to third parties. Plaintiffs allege that JetBlue breached that promise, thereby causing injury.

. . .

With regard to the existence of a contract, plaintiffs contend that JetBlue undertook a "self-imposed contractual obligation by and between [itself] and the consumers with whom it transacted business" by publishing privacy policies on its website or otherwise disclosing such policies to its consumers. Plaintiffs maintain that "these self-imposed public assurances ... created an obligation under the contract-of-carriage and a duty on the part of JetBlue and the persons with whom it did business not to act in derogation of JetBlue's privacy policy...." JetBlue counters that its "stand-alone privacy statement" — which "could only be accessed and viewed by clicking on a separate stand-alone link" on the bottom of JetBlue's website — is not a term in the contract of carriage. It further notes in this connection that "the entire transaction of purchasing transportation can be done on JetBlue's website (or by phone or in person) without ever viewing, reading, or relying on JetBlue's website privacy statement...." Although plaintiffs do allege that the privacy policy constituted a term in the contract of carriage, they argue alternatively that a stand-alone contract was formed at the moment they made flight reservations in reliance on express promises contained in JetBlue's privacy policy. JetBlue posits no persuasive argument why this alternative formulation does not form the basis of a contract.

JetBlue further argues that failure to allege that plaintiffs read the privacy policy defeats any claim of reliance. Although plaintiffs do not explicitly allege that the class members actually read or saw the privacy policy, they do allege that they and other class members relied on the representations and assurances contained in the privacy policy when choosing to purchase air transportation from JetBlue. Reliance presupposes familiarity with the policy. It may well be that some members of the class did not read the privacy policy and thus could not have relied on it, but the issue of who actually read and relied on the policy would be addressed more properly at the class certification stage. For purposes of this motion, the Court considers an allegation of reliance to encompass an allegation that some putative members of the class read or viewed the privacy policy. The Court recognizes that contrary authority exists on this point, but considers the holding in that case to rest on an overly narrow reading of the pleadings. *See In re Northwest*, 2004 WL 1278459, at *6 ("[A]bsent an allegation that Plaintiffs actually read the privacy policy, not merely the general allegation that Plaintiffs `relied on' the policy, Plaintiffs have failed to allege an essential element of a contract claim: that the alleged `offer' was accepted by Plaintiffs."). Accordingly, failure to specifically allege that all plaintiffs and class members read the policy does not defeat the existence of a contract for purposes of this motion to dismiss.

JetBlue also argues that plaintiffs have failed to meet their pleading requirement with respect to damages, citing an absence of any facts in the Amended Complaint to support this element of the claim. Plaintiffs' sole allegation on the element of contract damages consists of the statement that JetBlue's breach of the company privacy policy injured plaintiffs and members of the class and that JetBlue is therefore liable for "actual damages in an amount to be determined at trial." In response to JetBlue's opposition on this point, plaintiffs contend that the Amended Complaint is "replete" with facts demonstrating how plaintiffs were damaged , but cite to nothing more than the boilerplate allegation referenced above and another allegation in the Amended Complaint that they were "injured". At oral argument, when pressed to identify the "injuries" or damages

referred to in the Amended Complaint, counsel for plaintiffs stated that the "contract damage could be the loss of privacy", acknowledging that loss of privacy "may" be a contract damage. The support for this proposition was counsel's proffer that he had never seen a case that indicates that loss of privacy cannot as a matter of law be a contract damage. In response to the Court's inquiry as to whether a further specification of damages could be set forth in a second amended complaint, counsel suggested only that perhaps it could be alleged or argued that plaintiffs were deprived of the "economic value" of their information. Despite being offered the opportunity to expand their claim for damages, plaintiffs failed to proffer any other element or form of damages that they would seek if given the opportunity to amend the complaint.

The parties argued the issue of the sufficiency of damage allegations under New York state law. Based on this Court's review of the cited state authorities, it seems plain that had supplemental jurisdiction been declined and had the cases brought in New York proceeded in state court, the contract actions would have been dismissed based upon state pleading rules. *See Smith v. Chase Manhattan Bank, USA, N.A.*, 293 A.D.2d 598, 600, 741 N.Y.S.2d 100 (2d Dep't 2002) (allegation of contract damages consisting solely of "all to the damage of the class" is insufficient to support a claim for breach of contract); *Gordon v. Dino De Laurentiis Corp.*, 141 A.D.2d 435, 436, 529 N.Y.S.2d 777 (1st Dep't 1988). Neither side has addressed whether the result would be the same or different under the pleading requirements of Rule 8 of the Federal Rules of Civil Procedure, which in fact applies to this proceeding. *See* Charles A. Wright & Arthur R. Miller, Federal Practice and Procedure § 1204 (3d ed. 1998 & Supp.2005). Even if federal pleading rules require less specification, the result should not be different.

It is apparent based on the briefing and oral argument held in this case that the sparseness of the damages allegations is a direct result of plaintiffs' inability to plead or prove any actual contract damages. As plaintiffs' counsel concedes, the only damage that can be read into the present complaint is a loss of privacy. At least one recent case has specifically held that this is not a damage available in a breach of contract action. *See Trikas v. Universal Card Services Corp.*, 351 F.Supp.2d 37, 46 (E.D.N.Y.2005). This holding naturally follows from the well-settled principle that "recovery in contract, unlike recovery in tort, allows only for economic losses flowing directly from the breach." *Young v. U.S. Dep't of Justice*, 882 F.2d 633, 641 (2d Cir.1989) (citations omitted); *see Katz v. Dime Savings Bank, FSB*, 992 F.Supp. 250, 255 (W.D.N.Y.1997) (non-economic loss is not compensable in a contract action).

Plaintiffs allege that in a second amended complaint, they could assert as a contract damage the loss of the economic value of their information, but while that claim sounds in economic loss, the argument ignores the nature of the contract asserted. Citing the hoary case of *Hadley v. Baxendale*, the Second Circuit reminded the parties to the case before it that "damages in contract actions are limited to those that `may reasonably be supposed to have been in the contemplation of both parties, at the time they made the contract, as the probable result of the breach of it.'" *Young*, 882 F.2d at 641 n. 9 (quoting *Hadley v. Baxendale*, 9 Ex. 341, 156 Eng.Rep. 145 (1854)). A similarly basic principle of contract law is that the "purpose of contract damages is to put a plaintiff in the same economic position he or she would have occupied had the contract been fully performed." *Katz*, 992 F.Supp. at 255. Plaintiffs may well have expected that in return for providing their personal information to JetBlue and paying the purchase price, they would obtain a ticket for air travel and the promise that their personal information would be safeguarded consistent with the terms of the privacy policy. They had no reason to expect that they would be compensated for the "value" of their personal information. In addition, there is absolutely no

support for the proposition that the personal information of an individual JetBlue passenger had any value for which that passenger could have expected to be compensated. It strains credulity to believe that, had JetBlue not provided the PNR data en masse to Torch, Torch would have gone to each individual JetBlue passenger and compensated him or her for access to his or her personal information. There is likewise no support for the proposition that an individual passenger's personal information has or had any compensable value in the economy at large.

Accordingly, plaintiffs having claimed no other form of damages apart from those discussed herein and having sought no other form of relief in connection with the breach of contract claim, JetBlue's motion to dismiss the claim is granted. . . .

CHRIS PETERSEN, LOSING FACE
AN ENVIRONMENTAL ANALYSIS OF PRIVACY ON FACEBOOK

In 2006, two students at the University of Illinois were urinating on the front of a bar. When a police officer approached, Marc Chiles escaped while Adam Gartner was detained. Gartner denied knowing Chiles. Later, the officer accessed Facebook and scoured student profiles. When he realized Chiles and Gartner were Friends on Facebook the officer charged the latter with obstruction of justice. "I had no idea that old people were wise to Facebook," Gartner said. "I thought they referred to it as a doohickey that kids play with. I got bone-crushed." The director of public safety at the University of Illinois later said "[my] feeling about Facebook is, don't post anything you wouldn't want your mother or your future employers reading or seeing."

In 2007, the Daily Mail published dozens of photos of intoxicated college girls. "Drunkenly dancing on tables or collapsing in the street used to be a source of acute embarrassment for young women the morn- ing after the night before," crowed the tabloid. "Today, they are more likely to boast about it—to the world, with pictures—on social networking sites." The photos had been culled from a Facebook group called "30 Reasons Girls Should Call It A Night." One student pictured, taken by surprise as she had not posted the photos herself, found herself beleaguered by calls from overseas organizations offering money for sexually explicit interviews. A Google search of this student's name still returns the Daily Mail article as the first result.

In 2008, Katherine Evans was a high school student in Florida. Frustrated by a teacher's alleged unwillingness to assist her with schoolwork, Evans created a Facebook group dedicated to "hating" the teacher. After a few days and in a more temperate mood, she deleted the group. Two months later, she was suspended for "cyberbullying" the teacher. Evans is currently suing the school district, arguing that the suspension breached her rights and blemishes her record. Evans' experience recalls that of Cameron Walker, the president of Fisher College student government, who was expelled after he "damaged the reputation" of a campus police officer by joining a Facebook group critical of the officer's treatment of students.

In 2009, a 16-year-old employed by a marketing firm in England returned home from work and wrote on her Facebook that her job was "boring." She was promptly fired after colleagues accessed her profile and passed on the post to her supervisor. "[This] display of disrespect and dissatisfaction undermined her relationship with the company," a representative of the firm said. "Had [she] put up a poster on the staff notice board making the same comments and invited other staff to read it there would have been the same result." Skeptics argued that employers

rarely followed their employees to the local bar to eavesdrop on any griping that regularly occurred there.

By 2009 many students found themselves in the uneasy position of having to decide whether to Friend parents or others outside the college context. "Alright im just gonna put this out there. . . It is really weird that Adults are on facebook!!" wrote Jess, a college senior. When asked why it was "weird," she elaborated "because my moms friends are n facebook. . . its jsut weird. and they also do it to watch every moment of there kids life and not give them privacy." Another student reported that "the whole system feels wrong. I can't ignore a 'friend request' from the mother of my girlfriend, sure she's great in real life, but I want to keep that part of my life separate from my life I shared with folks in college. . . It's odd, but it's like I'm too connected." These concerns and complaints echo those of Rachel, who trusted her grandmother but nevertheless felt uncomfortable exposing every aspect of her college experience to someone outside the college context.