Parallel-Effect Statutes and E-Mail "Warrants": Reframing the Internet Surveillance Debate

Paul K Ohm*

Introduction

The public debate about Internet surveillance seems one marked by deep divisions in fundamental values. The two sides of this debate appear separated by a deep and growing chasm, one side waving the banner of privacy and freedom, the other side trumpeting security and accountability. As most of the parties to the debate will probably admit, the chasm between the sides is not so wide, and many bridges of common concern span the gap. We all want the Internet to be a safer, freer place to communicate, and we all acknowledge that we must accept certain costs and sacrifices to help bring that Internet about. Ours is a search for the proper balance between privacy and security. I believe these divisions have been the focus of too much attention because the parties have spent most of the debate fighting their battles in the trenches, butting heads over picayune specific details in statutory text that rarely, by themselves, impact safety or privacy. The purpose of this Article is to recast the debate from one level up: Can we develop sound procedures or prophylactic measures to ensure privacy and security, even if we cannot agree today on the specific substantive form that our Internet surveillance laws should take?

Reasonable minds may differ about substantive Internet surveillance questions. Here is an example: What parts of an Internet communication are "content"—and thus regulated by Title III—and what parts are "non-content"—and thus protected by the pen register, trap and trace statute? Odds are that a government prosecutor would draw that line in a different place than a defense attorney defending a client against computer crime charges.

It might be difficult and frustrating, then, to redraw all of our statutory lines at this Symposium. Instead, in this Article, I critique the current debate and then try to identify a few modest reforms with which all sides may be able to agree, consistent with their differences in vantage point. In Part I, I argue that the current debate over Internet surveillance laws takes place in an information vacuum; we do not know enough about the effect of our laws on privacy or security. Lacking information, we are left guessing about whether our surveillance capabilities need to be expanded or contracted and, in support of these guesses, slinging anecdotes and platitudes. In Parts II and

* Trial Attorney, Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice. Former law clerk to Betty Binns Fletcher, United States Court of Appeals for the Ninth Circuit, and Mariana Pfaelzer, United States District Court for the Central District of California. J.D., UCLA School of Law, and B.S. in Computer Science, Yale University. Mr. Ohm participated in the Symposium in his personal capacity, and the views articulated in this Article do not necessarily reflect the views of the Department of Justice.

August 2004 Vol. 72 No. 6

III of this Article, I propose changes to surveillance law that focus on procedural and prophylactic improvements to the law, instead of ultimate substantive standards. Specifically, in Part II, I analyze a self-policing mechanism—the parallel-effect statute—that has not been extensively discussed in the literature. In Part III, I argue that we should revamp a specific procedure in the Stored Communications Act ("SCA").[1] Changes such as these can build protections into the law and help us gather the type of information we need in order to do more than merely shout past one another.

I. A Critique of the Current Debate

Calls to change Internet surveillance law come in three flavors that I label "substantive," "procedural," and "prophylactic." A substantive fix is a call to redefine the categories of Internet surveillance or alter the standard of proof assigned to each. For example, a classic substantive distinction in the law is that Title III, the Wiretap Act,[2] governs prospective surveillance, meaning the contemporaneous interception of electronic communications,[3] while the SCA governs access to static, historical information, such as stored file transfer protocol ("ftp") log files.[4] Absent a statutory exception, the government must have probable cause before it can do the former[5] and introduce at least "clear and articulable facts" of "relevan[ce] and material[ity]" before it can access the latter.[6] A call to redraw the line between the categories of surveillance or to raise or lower these standards of proof would be an example of what I am calling a substantive fix.

A procedural fix would alter the procedures that the government must follow before it may access communications; an example is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act")[7] change that enabled government agents to apply for a § 2703(a) probable cause order/warrant in one federal district court that could be served on an Internet service provider ("ISP") in the jurisdiction of another district court.[8]

Finally, prophylactic recommendations are those that encourage law enforcement to comply with the rules or provide for greater legislative and judicial oversight of those rules. Statutory suppression is an example of a

---

1 18 U.S.C.A. §§ 2701–2712 (West 2003). Consistent with the convention chosen by Orin Kerr in this Symposium, I refer to Chapter 121 of Title 18, formally entitled "Stored Wire and Electronic Communications and Transactional Records Access," as the "Stored Communications Act," or "SCA." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 n.1 (2004).

2 18 U.S.C.A. §§ 2510–2522 (West 2003). Title III refers to Chapter 119 of Title 18. The chapter was first enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

3 *See id.* §§ 2511, 2518.

4 *See* 18 U.S.C.A. § 2703(c).

5 *See* 18 U.S.C.A. § 2518(3).

6 *See* 18 U.S.C.A. § 2703(c).

7 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

8 *See id.* § 220, 115 Stat. at 291. I choose the awkward locution, "probable cause order/warrant," purposefully for reasons that I explain in greater detail in Part III, *infra*.

prophylactic recommendation that has been raised more than once at this Symposium.[9]

People focus too often on substantive fixes when their concerns suggest procedural or prophylactic alternatives. Often, the wiser route is the procedural or prophylactic fix because it is much more likely to become law. The substantive categories that separate different types of Internet surveillance have evolved through several decades; the standards of proof that the government must meet before it can engage in one kind of surveillance or another have a similarly developed pedigree. The substantive law has reached something of a steady state through compromise and the voiced input of interested parties on many sides of the debate. Obviously, this is not to say that the process is finished, the statutes set in stone; the perception persists, right or wrong, that Internet privacy is currently underprotected and undervalued. Meanwhile, law enforcement continues to press for new tools to fight crime and ensure security. The debate rages onward.

A fundamental flaw in the debate is that far too much of it rests on platitudes and anecdotes. Empty platitudes, of course, are worthless. For every empty maxim about the threats that exist on our networks ("Every day, a digital Pearl Harbor strikes somewhere in America."),[10] there is a competing aphorism about the threat to online privacy (inscription on a website-based tombstone referring to the USA PATRIOT Act: "The Fourth Amendment: 1789–2001").[11]

Anecdotes, while more useful than empty platitudes, likewise skew the debate. For example, both sides have misused court precedent in anecdotal arguments. The routine has played out many times: some federal district court judge issues an opinion that one side of the Internet surveillance debate finds threatening and outrageous; this group uses the court opinion to lobby Congress and the public for a change. No one seems to notice or care that the opinion is an outlier, seriously out-of-step with national trends, and likely to be reversed by the court of appeals. The rhetoric is so effective that Congress—and sometimes even the public—rallies against it; the statute is changed, a mere year or two after the most recent overhaul of the very same provision. This "siege overreaction" mentality arises because case law develops so sporadically in this field that partisans give unwarranted weight to the little that emerges.[12]

The parties to the debate resort to anecdotes and platitudes because they do not have enough information about the level and quality of privacy that exists and the type of security that is desired, necessary, or attainable. Lacking information, advocates talk past one another with one group recom-

---

9 Kerr, *supra* note 1, at 1241; Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1285 (2004).

10 This statement is both untrue and disrespectful to victims of the actual Pearl Harbor attack.

11 *See* Patricia Cohen, *9/11 Law Means More Snooping? Or Maybe Less?*, N.Y. TIMES, Sept. 7, 2002, at B9.

12 *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 823–24 (2003) (discussing the paucity of case law in the area of electronic surveillance).

mending a sweeping substantive change to bolster privacy, another recommending the maintenance of the status quo, and a third side trying to expand surveillance powers dramatically. How is a conscientious legislator or judge to decide? Whom should the public believe?

Faced with this void of information, the solution is not dramatic change in the categories or standards of proof. With patience, we will collect and process more information over time through experience and case law. Better yet, while we wait, we can create statutory mechanisms to shine light on how the system is working; the system needs better transparency. Transparency can take many forms: more judicial oversight (transparency *vis-a-vis* courts),[13] additional reporting requirements (transparency to Congress and the public),[14] or increased notice requirements (transparency to targets and defendants).

What should these light-shining mechanisms look like? Below, I recommend two specific changes of the kind that have not, in my opinion, been discussed enough. One of my recommendations is prophylactic, the other procedural. My prophylactic recommendation, discussed in Part II, is to write statutes that encourage law enforcement agencies to engage themselves more often in the privacy-versus-security debate by using a statutory technique—the parallel-effect statute—that has not been discussed much in the literature. My procedural recommendation, in Part III, is to revise and revamp a particular procedural tool in the SCA, the § 2703(a) warrant.

II. Law Enforcement Self-Policing by Design: Parallel-Effect Statutes

A. Statutes That Encourage Self-Policing

Many have expressed concern that, in the current Internet surveillance scheme, law enforcement agencies lack accountability. We cannot trust our police officers, agents, and prosecutors to obey the law, the argument goes, because they have no incentive to obey it and because they are so rarely held accountable for violating it. Those who voice this concern are often arguing for increased statutory suppression remedies or more judicial and legislative oversight. I suggest that another, in many ways better, accountability enhancing scheme has been overlooked in the literature and recommend that we apply this scheme, when possible, to other statutes.

Title III, the Wiretap Act, possesses a self-policing mechanism that has served as an effective check on law enforcement overreaching.[15] The Wire-

---

13 During the process leading up to passage of the USA PATRIOT Act, Senator Leahy proposed a more rigorous judicial review over applications for pen register and trap and trace device orders. Beryl Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1157 (2004). The Department of Justice countered that the then-existing standard struck the correct balance between privacy and security; the Department's view won the day. *Id.*

14 *See, e.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288–90 (requiring mandatory government reporting to the court when the government uses "its own pen register or trap and trace device," such as DCS-1000/Carnivore).

15 *See* 18 U.S.C.A. §§ 2510–2522 (West 2003).

tap Act is a multiheaded hydra: it serves both as a criminal prohibition against illegal interception and as a set of rules governing lawful interception. Section 2511 sets out a prohibition—"thou shall not unlawfully intercept"[16]—a prohibition for "any person" that applies with equal force to agents investigating crime and to ordinary citizens listening in on their neighbors. Section 2511 also provides exceptions to that rule: "Thou may intercept in certain situations."[17] Many of these exceptions apply to all people, whether or not they happen to wear a badge.[18] Court rulings construing these exceptions in one context are applied with equal force to all others.

This dual-headedness serves as a powerful internal check. If law enforcement agents seek to "push the envelope" in their interpretation of the statute to justify their investigative techniques, they will be forced to live with the same interpretations when they pursue criminal wiretappers. A vast expansion in the definition of criminal wiretapping leads to a vast contraction in the definition of the law enforcer's wiretapping ability; the two are inversely proportional. And, here is where something remarkable and perhaps unintended happens: law enforcement must engage in an internal debate in search of a balance. The debate favors moderation, and overly aggressive legal theories will not be pursued when at odds with positions or practices taken by another side of the house.

Imagine that police officers in a jurisdiction at the End of the Universe have been debating whether they need to seek court process to use the Zaphod Beeblebrox, the newest type of surveillance technology. The ZB, as it is known to those in the know, can intercept words typed on a computer keyboard, from ten miles away, and five minutes before the words are actually entered. "Imagine the benefits to law enforcement!" police officers exclaim. "Crimes can now be detected and stopped, before they ever occur."

At some point in the future, the fact that the ZB exists and has been used by the police will come to public light. But until that day, the police will have an incentive to keep its use under wraps. And without public knowledge, nobody will be able to debate the police about the effect of ZB on Internet privacy and security, except for others within the police department. The prospect of an internal debate might seem unlikely were it not for the structure of the Wiretap Act. Because, imagine further that an ordinary citizen, living in the same jurisdiction at the End of the Universe, has built his own version of the ZB and uses it to eavesdrop on his neighbor's communications. The police department, deciding whether to charge this citizen, will

---

16 *See id.* § 2511(1) ("[A]ny person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).").

17 *See, e.g., id.* § 2511(2) (listing exceptions).

18 Some exceptions apply only to law enforcement. *See, e.g., id.* § 2511(2)(c) (consent of a party for monitoring by person "acting under color of law"). Some exceptions apply only to non–law enforcement. *See, e.g., id.* § 2511(2)(d) (consent of a party for monitoring by person "not acting under color of law"). Others apply only to certain governmental entities. *See, e.g., id.* § 2511(2)(b) (exception for monitoring responsibilities of the Federal Communications Commission). Still others apply only to providers like ISPs and phone companies. *See, e.g., id.* § 2511(2)(a)(i) (provider-protection exception).

face a quandary. If the citizen is charged with criminal wiretapping, the prosecutor will need to make arguments which, if adopted as correct interpretations of the law, will also call into question the police department's ability to use the ZB without a Title III order. If the police do not charge the citizen, the police will remain free to use the ZB without process, but a person who may deserve punishment will go free. Do unto others as you would have the courts interpret the law to do unto you.

I have seen this debate in action, and I honestly believe that it has helped strike a balance between security and privacy in the application of Title III. Neither goal will likely be sacrificed for the other, except when merited by extreme circumstances.

Critics will no doubt suggest that law enforcement agents will sacrifice one half of their mission to better serve the other. They will probably argue that the police will let wiretappers remain free if it means that investigating crime will be easier. This does not seem to be the case. At least in the federal law enforcement community, wiretapping is seen as significantly antisocial behavior that should be prosecuted vigorously. The law enforcement community touts its aggressive prosecutions of these criminals. In computer crime cases, § 2511 is an important tool to the prosecutor, providing a federal felony in some cases where otherwise only federal misdemeanors have been committed. Insiders who deploy "sniffers," or criminals who monitor incoming e-mail messages, may have committed no other crime except § 2511 violations.

This internal check is not meant to replace judicial and legislative oversight; it is simply an underdiscussed, built-in check on executive power. In some ways, this check is superior to judicial and legislative techniques. When law enforcement agents try to decide whether privacy (use of the ZB without an order violates Title III) or security (use of the ZB without an order does not violate Title III) should prevail in a given situation, they are engaged in the same debate that we are participating in at this Symposium. In contrast, courts are usually faced with a particular fact pattern that presents only half of the debate. "The defendant used this technique and should be punished" or "the police officer used this technique and, thus, this evidence should be suppressed." The privacy-versus-security debate is not cast into sharp relief. Furthermore, in court, the government will often not be willing or allowed to air the internal debate before the judge and defense counsel. Worse yet, the lone government lawyer, vigorously litigating for the prosecution, may not understand the full effect of the arguments he is advancing.[19]

Legislatures may move too slowly to respond to developments in technology. In contrast, law enforcement in debate with itself can engage in a continuous, constant, and ever-changing contest that nimbly keeps up with changes in technology and does not wait for the legislative cycle or shift with the political winds.

---

19 Note that all of these problems (and more) are compounded greatly when the government is not involved at all in the case. Civil litigants, advancing their positions, often convince judges to issue opinions that sow confusion into criminal Internet surveillance law. *See generally* Kerr, *supra* note 12, at 829–30.

B. Other Self-Policing Internet Surveillance Laws

Unfortunately, this type of check cannot be applied to every statute that bears on Internet surveillance. Many Internet surveillance statutes currently lack the parallelism of the Wiretap Act; sometimes we do not care if the average citizen can do something; we just do not want the police to be able to do it, or even when we do not want *anybody* to do something, we may care much more that the police not do it. For example, look at the voluntary disclosure rules of the SCA. Title 18, § 2702(c)(6) allows ISPs to disclose any records or information "pertaining to a subscriber or customer," aside from the contents of communication, "to any person other than a governmental entity."[20] ISPs can disclose this kind of noncontent information to governmental entities only if they fall within the exceptions listed in the other subsections of § 2702(c). This provision is why the network administrator of ISP A can provide the name of a user associated with particular network activity to the network administrators of Company A without fear of liability under the SCA. These same ISP network administrators, on the other hand, cannot disclose user-specific information to the government, unless one of the exceptions listed in § 2702(c) applies.[21]

Other provisions work the opposite way: we may not want the general public to be able to do something, but we allow the police to do it, usually with careful oversight. As an example, take the preservation requirement of § 2703(f). According to this provision, an ISP must preserve any records in its possession, when the government requests it, for at least ninety days.[22] This legally obligates the ISP to comply with the request. This power is not available to the general public. Members of the general public may ask an ISP to preserve records, but the ISP receiving the request is under no obligation to comply.

Another class of statutes that empower the government and not private parties are provisions that identify the legal process that law enforcement can use to conduct surveillance, such as § 2518 (Title III Orders), § 2703 (SCA warrants, orders, and subpoenas), and § 3123 (Pen Register and Trap and Trace orders) of Title 18. Only the government is empowered to obtain these types of legal process. These statutes lack the parallelism described above.

Finally, there are the "parallel-effect statutes," provisions that, like Title III's prohibition on interception, apply equally to the government and the public. Let us focus on two other similar provisions. First, § 3121 of the pen

---

20 *See* 18 U.S.C.A. § 2702(c)(6) (West 2003). To be precise, § 2702 applies to public providers of "electronic communications service," which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications," 18 U.S.C.A. § 2510(15), and to providers of "remote computing service," which is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system," 18 U.S.C.A. § 2711(2).

21 *See id.* Notice, however, that the prohibitions on voluntary disclosure in the SCA apply only to providers *to the public*. *See id.* § 2702(a). *Nonpublic* providers, such as employers, are not covered by these provisions. They can volunteer any information about their users, including the content of communications, to anyone, for any reason, without violating the SCA. *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998).

22 18 U.S.C.A. § 2703(f)(2). This ninety-day time period may be extended upon a "renewed request." *Id.*

register, trap and trace statute is structured like the wiretap statute: it prohibits the actions of the government and of everyone else as well. Nobody—not private sysadmins and not the police—may install or use a device to record or decode the dialing, routing, addressing, and signaling information of others' communications unless they fall within an exception to the statute.[23]

Another parallel-effect provision can be found in the SCA, although it is trickier to locate. The parallelism stems from the definition of "electronic storage" in § 2510(17). "Electronic storage" is defined, in part, as the "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[24] The parallelism surrounding "electronic storage" is found in two parts of the SCA. First, if items in "electronic storage" are obtained, altered, or blocked by a person accessing a mail server without authorization, that person has committed a crime.[25] In a completely separate part of the SCA, the government is given the power to compel a provider to disclose an item "in electronic storage" only with a warrant.[26]

We thus see a parallelism similar to the Title III parallelism: if "electronic storage" is broadly construed, more unauthorized intruders can be prosecuted for violating § 2701(a), but the government can obtain fewer types of communication with less than a warrant. If "electronic storage" is narrowly construed, the government may compel the production of a larger class of information from an ISP with something less than a warrant, but fewer crimes will be available to be prosecuted.

C. Parallel-Effect Statutes and Legislatures

Congress and state legislatures can build a parallel-effect structure into many types of Internet surveillance statutes. Anytime Congress seeks to limit the government's access to particular types of communications, it should ask itself whether to create a parallel criminal prohibition applicable to "any person." If the behavior is of the kind that all people should be proscribed from doing, a parallel-effect statute makes sense.

Congress may also revisit statutes that already have parallel-effect structures but lack the balance needed to foster a vigorous debate. For example, the pen register and trap and trace statute is structured nearly identically to the Wiretap Act—18 U.S.C.A. § 3121 defines both a criminal prohibition and a limit on law enforcement use[27]—so we would expect to see the same kind of internal debate and the concomitant balancing of security and privacy as we have with the Wiretap Act. On the contrary, very few people are ever charged with violating the pen register, trap and trace statute.

The reason for this difference is that the police are probably not worried about losing the ability to bring the few pen register, trap and trace cases that might be brought each year by aggressively pursuing a new surveillance tech-

---

23 18 U.S.C.A. § 3121.

24 18 U.S.C.A. § 2510(17)(A).

25 18 U.S.C.A. § 2701(a).

26 *Id.* § 2703(a).

27 18 U.S.C.A. § 3121.

nique.[28] The internal check seems to be missing. One recommendation to strengthen the internal check is to give the police a reason to care more about this crime, for example, by making it a federal felony instead of a misdemeanor.[29] If this were done, the police might investigate and charge more pen register or trap and trace crimes, which would more frequently lead to the balancing described above.[30]

In fact, stronger punishments have recently been added to the parallel-effect provision of the SCA described above: the criminal prohibition in § 2701(a) for those who obtain or alter communications in electronic storage. Prior to the passage of the Homeland Security Enhancement Act of 2002 ("HSEA"),[31] first time violators of § 2701(a) faced a maximum one-year misdemeanor charge.[32] Section 225 of the HSEA—the so-called "Cyber Security Enhancement Act"—elevated the crime in some cases to a five-year felony, ten years for repeat offenders.[33]

Prosecutors are very likely to begin charging this statute, which has always been a bit of a neglected stepchild for computer crime prosecutors. As vigorous and novel theories of criminal liability are fit into § 2701(a), prosecutors will be kept in check by the effect that their novel interpretations have on the definition of "electronic storage" and thus on the compelled production aspects of § 2703.[34]

D. Parallel-Effect Statutes and the Courts

Courts interpreting parallel-effect statutes should take into account the effect that their rulings will have in the statute's other context. Will construing a statute narrowly to reverse the conviction of a defendant broaden the government's ability to conduct surveillance without a court order? Does the acceptance of a broad jury instruction that makes a conviction more likely mean that the government will find it much more difficult to conduct future surveillance?

Legal scholars have made a similar recommendation with respect to statutes and rules that provide both civil and criminal remedies for violations, such as Rule 10b-5 promulgated by the Securities and Exchange Commission.[35] According to these scholars, courts construing civil–criminal hybrid

---

28 I am not trying to suggest that the police neglect the pen register, trap and trace statute. My experience has been that they take their requirements quite seriously. Of course, this is simply an anecdotal assertion.

29 *See* 18 U.S.C.A. § 3121(d) (one-year penalty for violations).

30 The obvious problem with this recommendation is that we, as a society, may not care enough about nongovernmental pen register and trap and trace abuses to call them felonies. Maximum sentences reflect societal assessments or punitive and rehabilitative goals and have not traditionally been thought of as a way to discipline parallel police behavior.

31 Homeland Security Enhancement Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135.

32 18 U.S.C.A. § 2701(b)(1) (providing a maximum sentence of "not more than one year" when "the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain").

33 Homeland Security Enhancement Act of 2002 § 225(j)(2).

34 *See supra* Part II.B.

35 *See* 17 C.F.R. § 240.10b-5 (2004); Margaret V. Sachs, *Harmonizing Civil and Criminal Enforcement of Federal Regulatory Statutes: The Case of the Securities Exchange Act of 1934*,

statutes in their differing contexts can reach differing interpretations, and differing interpretations are to be avoided.[36] Divergence is to be disfavored for many reasons, some of which apply also to parallel-effect statutes. First, Congress wrote these statutory hybrids using a single set of definitions and other common language, and these congressional choices should be respected.[37] Second, consistency obeys the canon of statutory construction that language in a statute has a consistent meaning throughout.[38] Finally, "multiple constructions of a single prohibition are likely to be unstable."[39]

To achieve a single, consistent interpretation, courts should invoke what one scholar calls the "all contexts" rule.[40] To seek the one correct, consistent interpretation:

> [C]ourts should not focus solely on the immediate enforcement context. Rather, they should . . . consider every action to enforce the prohibition under the hybrid statute and the policies pertinent to each. If the policies conflict, courts should seek the most appropriate compromise.[41]

A Title III case that is currently on appeal involves a legal issue that should be viewed under the all contexts rule. In *United States v. Councilman*, a federal criminal case arising out of Massachusetts, the defendant ran an e-mail listserv that catered to collectors of rare books.[42] Defendant offered accounts that could be used to receive e-mail messages to some customers.[43] Unbeknownst to them, some of the messages sent to these accounts were allegedly intercepted by the defendant.[44] Using this scheme, the defendant could allegedly monitor private communications between Amazon.com and his customers, which may have given him a competitive advantage.[45] In 1999, representatives of the defendant's company pled guilty to violating the Wiretap Act and paid a $250,000 fine.[46]

An important issue raised in *Councilman* was whether this scheme amounted to a wiretap in violation of Title III.[47] The district court held that it did not because, according to stipulated facts, the e-mail messages were "in

---

2001 U. ILL. L. REV. 1025, 1028; Lawrence M. Solan, *Statutory Inflation and Institutional Choice*, 44 WM. & MARY L. REV. 2209, 2238–40 (2003).

36 *See* Sachs, *supra* note 35, at 1033 ("[C]ourts should limit prohibitions in hybrid statutes to a single interpretation.").

37 *See id.* at 1031 ("There is no basis for supposing—without more—that Congress expects courts to abrogate its choice of statutory form by means of construction.").

38 *Id.* at 1032 (finding that the reason "extrapolates from the well-established presumption that language appearing repeatedly in a statute has one meaning throughout.").

39 *Id.* at 1033.

40 *Id.* at 1033–34.

41 *Id.*

42 United States v. Councilman, 245 F. Supp. 2d 319, 320 (D. Mass. 2003); *see* Posting of Orin Kerr, okerr@law.gwu.edu, to http://hermes.circ.gwu.edu (Feb. 19, 2003) (copy on file with The George Washington Law Review).

43 *See Councilman*, 245 F. Supp. 2d at 320.

44 *See id.*

45 Book Seller Illegally Intercepted Emails, REUTERS, ¶ 3 (Nov. 23, 1999) (on file with The George Washington Law Review).

46 *See id.*

47 *See Councilman*, 245 F. Supp. 2d at 320.

storage" when they were acquired.[48] At various points in its opinion, the district court explained that data in storage, no matter how "ephemeral," and even if lasting just for a "nanosecond," cannot be "intercepted" under Title III.[49]

The district court's holding that the defendant's actions did not constitute a Title III violation has been appealed to the United States Court of Appeals for the First Circuit.[50] In addition to the traditional statutory construction arguments that the parties will likely raise on appeal, the First Circuit may choose to consider the parallel-effect structure of Title III. If the defendant's acts did not violate Title III, the government could conduct the very same kind of surveillance without needing to satisfy the heightened requirements of that statute.[51] Currently, the government seeks a full Title III order to conduct any contemporaneous, real-time, and ongoing acquisition of e-mail messages.[52] If the district court is upheld, then a § 2703(a) warrant would be all that is required. Any warrant, and in particular a § 2703(a) warrant, is significantly easier for the government to obtain than a Title III order. The effect of the *Councilman* district court ruling would be to decrease greatly the privacy afforded e-mail communications.

The First Circuit should therefore consider "all contexts." In addition to weighing the privacy rights of the rare book dealers whose e-mail messages may have been read by the defendant, the court should consider the effect of its decision on the privacy rights of private citizens *vis-a-vis* the government.[53]

---

48 *See id.* at 321. Note that the district court sometimes uses the phrase "storage" instead of the proper statutory phrase "electronic storage." *Id.* The two phrases do not mean the same thing. *See* 18 U.S.C.A. § 2510(17)(A) (West 2003).

49 *See Councilman*, 245 F.Supp. 2d at 321.

50 On June 29, 2004, as this Article was entering the final stages of the editing process, the First Circuit decided *United States v. Councilman (Councilman II)*, 373 F.3d 197 (1st Cir. 2004). In a split decision, the First Circuit affirmed the district court's dismissal of the Indictment.

51 *See* Posting of Orin Kerr, *supra* note 42 ("If adopted by other courts, it will mean that the government could conduct virtual wiretaps without having to comply with the Wiretap Act. Just program a Carnivore-like sniffer to collect traffic a "nanosecond" after it arrives, and no need to get a wiretap order—an ordinary search warrant will do.").

52 *See id.* ("The government doesn't actually want this authority—note that the government was arguing *against* this construction in Councilman—but it's something the court's opinion would allow.").

53 The majority opinion affirming the district court's decision devotes almost no attention to "all contexts" analysis. The majority discusses neither the government's use of monitoring technology in its law enforcement role nor the impact that its decision may have on the privacy of the citizenry from police invasion. The opinion does tip its hat at this type of reasoning, concluding that "[i]t may well be that the protections of the Wiretap Act have been eviscerated as technology advances." *Councilman II*, 373 F.2d at 203. Despite this acknowledgement, the majority opinion never discusses whether law enforcement's use of this technology can be considered to help decipher the legislative intent underlying the statute.

In contrast, Judge Lipez in his much longer dissent devotes an entire section, Section V, to the "all contexts" problem. *Id.* at 218–19. After spending the bulk of the dissent describing why he disagrees with the majority's interpretation of the plain language, legislative history, and precedents, Judge Lipez discusses how the government may profit from the majority's conclusion. In sum, "[u]nder Councilman's narrow interpretation of the act, the Government would no longer need to obtain a court-authorized wiretap order to conduct surveillance. This would effectuate a dramatic change in Justice Department policy and mark a significant reduction in the

E. Encouraging the Debate Through Organizational Structure

Finally, the efficacy of the internal debate that emerges from parallel-effect statutes may depend on the number and nature of the competing parties involved. If a law enforcement agency—say, the Department of Justice—charges one small unit both with deciding what investigatory tools may be used consistent with Title III and with pursuing criminals who commit illegal wiretaps, the debate will be held on a small scale, among a small cadre of familiar colleagues. There are advantages and disadvantages to this structure: a smaller group can better predict the effects that their arguments will have on the "other side" of the house, but the debate may lack the vigor that truly adversarial parties can bring.

On the other hand, if two very distinct groups on opposite ends of the organizational chart are tasked with the sides of this debate—one an investigatory techniques unit, the other a wiretap prosecuting unit—the risk is that neither side will know what the other is doing, but the benefit is that the two sides will come to the debate more as arms-length adversaries. Disagreements between the sides will be resolved organizationally by a more highly ranked, and often more politically accountable, Department official who will make the ultimate decision.

III. Section 2703(a) Orders (Also Known as Warrants)

As provided in the SCA, the government can compel the production of content (e-mail messages, other files) and noncontent (logfiles, credit card billing records) from certain types of ISPs if they first obtain the correct type of process.[54] Three types of process are described in the statute: warrants,[55] 2703(d) orders,[56] and subpoenas.[57] Much of the commentary about the SCA has focused on where to draw the substantive lines between the three types of process.[58] The focus is often on whether a warrant or a 2703(d) order is required to obtain a particular type of file. The stakes are significant because the answer defines in very broad strokes how high a hurdle the government must clear and thereby defines the privacy of our stored communications.

Under the SCA, law enforcement officials must seek a "warrant" before they can compel ISPs to produce a user's unopened or never retrieved electronic mail messages.[59] These "warrants" are not like the search warrants used in the physical world: they are "executed" when a law enforcement

---

public's right to privacy." *Id.* at 219. Judge Lipez's dissent is a paradigm of the type of careful, "all contexts" analysis for which I call in this Section.

54 *See* 18 U.S.C.A. §§ 2701–2712 (West 2003). The rules are complex and will not be described in full in this Article. For more complete treatment, see U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS Ch. III (2002), http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm; *see also* Kerr, *supra* note 1, at 1218–20.

55 18 U.S.C.A. § 2703(a), (b)(1)(A), (c)(1)(A).

56 *Id.* § 2703(b)(1)(B)(ii), (c)(1)(B), (d).

57 *Id.* § 2703(b)(1)(B)(i), (c)(2).

58 Solove, *supra* note 9, at 1266 (advocating a probable cause standard for government access to "most uses of electronic surveillance").

59 18 U.S.C.A. § 2703(a).

agent delivers (sometimes by fax) the warrant to the ISP. The ISP, not the agent, performs the "search"; the ISP "produces" the relevant material to the agent; the user associated with the inbox often never learns that his inbox has been "searched." In sum, these are not search warrants at all and to call them such confuses legal terminology. Congress should amend SCA to reflect what they really are, and I have a descriptive, if not particularly poetic, suggestion: "section 2703(a) probable cause orders."

But this is not a pedant's gripe about diction and linguistic purity. Although it may mollify people to think that their unopened e-mail is protected from government intrusion by a search warrant requirement, in practice, more harm than good may come to privacy by treating these orders as full-blown search warrants. When courts treat hybrid warrant-subpoenas using the rules designed for real-world search warrants, confusion reigns.

The problem stems from identifying the procedural rules that govern these warrant-subpoena hybrids. Regular, real-world search warrants are governed by at least three sources of positive, procedural law: Rule 41 of the Federal Rules of Criminal Procedure, §§ 3101–3118 of Title 18 of the U.S. Code, and the Constitution. These provisions provide a "procedural net" of rules that define, in fine detail, the steps that must be taken to obtain, execute, and return a search warrant. So, for example, unless specific authorization to do otherwise is granted, real-world search warrants must be executed in daytime hours because Rule 41(e)(2)(B) requires it.[60] Likewise, a court will issue a warrant for a real-world search only if police have shown probable cause because both the Constitution and Rule 41(d)(1) require it.[61]

Which rules from the procedural net apply to § 2703(a) warrants? Some of these rules, designed for physical searches of persons and places, have no meaning in the subpoena-like e-mail "search" context. A recently litigated example is the requirement of officer presence. According to 18 U.S.C. § 3105, "[a] search warrant may in all cases be served by any of the officers mentioned in its direction or by an officer authorized by law to serve such warrant, but by no other person, except in aid of the officer on his requiring it, he being present and acting in its execution."[62] Similarly, Rule 41(f) presupposes that an officer is "present during the execution of the warrant."[63] As a matter of fact, in the 2703(a) context, it is probably best for all involved if an officer is not present when the warrant is executed. Most ISPs do not want FBI agents rifling through their mail servers.[64] It is fair to assume that users do not want that either. Instead, the warrant is almost always sent via

---

60 "The warrant must command the officer to . . . execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time . . . ." FED. R. CRIM. P. 41(e)(2)(B). "'Daytime' means the hours between 6:00 a.m. and 10:00 p.m. according to local time." FED. R. CRIM. P. 41(a)(2)(B).

61 U.S. CONST. amend. IV ("no Warrants shall issue, but upon probable cause"); FED. R. CRIM. P. 41(d)(1).

62 18 U.S.C. § 3105 (2000).

63 FED. R. CRIM. P. 41(f)(2).

64 *See* Brief of Amici Curiae Yahoo!, Inc., the Computer & Communications Industry Association, NetCoalition and the United States Internet Service Providers Association In Support of Appellant United States of America and Urging Reversal at 5, United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (No. 02-1238), *available at* http://www.epic.org/privacy/bach/

fax to the ISP that is the subject of the warrant, and the ISP takes charge of finding the specified content and sending it to the officer.

The issue of officer presence arose in a recent case, *United States v. Bach*, and the resulting district court and court of appeals opinions highlight the difficulties inherent in applying real-world search warrant procedures to 2703(a) warrants.[65] In *Bach*, state police officers executed an SCA warrant by faxing a copy to Yahoo!.[66] A federal district court judge suppressed the evidence obtained, reasoning that the search violated the requirements of 18 U.S.C. § 3105's "officer presence" rule, which it held codified a Fourth Amendment requirement.[67] Violate 3105 and, in the district court's opinion, you violate the Fourth Amendment.

The court of appeals reversed, holding in no uncertain terms, "We disagree with the district court's determination that section 3105 codifies the Fourth Amendment's requirements for searches and seizures and agree with the Second Circuit that the inquiries under section 3105 and the Constitution are separate and distinct."[68] Although the court held that the presence of an officer can be considered by courts as part of the reasonableness test in the Fourth Amendment, it is not, by itself, dispositive of the question.[69]

Whether or not the court of appeals was correct about the *per se* constitutional dimension of the test in § 3105, the court was not in the proper position to assess the issue. A search warrant was not used in this case; a 2703(a) "warrant"—which should have been considered for these purposes to be a mere subpoena or court order—was used, and there is no reason why § 3105 should even have been consulted. Nevertheless, it is now enshrined in Eighth Circuit law that officer presence is not a requirement of the Constitution, and this conclusion is not at all limited to SCA warrants. If the police send a private party in their place to search a defendant's car, home, or office, the defendant is foreclosed from the argument that the Constitution has, *per se*, been violated, because the court's unequivocal pronouncement has put an end to the debate.[70]

The fact that § 3105 should not have even been in issue is demonstrated by the court's subsequent analysis of whether the "service" by fax of the SCA warrant violated the reasonableness requirement of the Fourth Amend-

---

band_amicus.pdf (last visited June 13, 2004) ("[A] physical presence requirement will disrupt the efficient operation of a service provider's business.").

65 United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002), *rev'g* No. 01-221, 2001 U.S. Dist. LEXIS 21853 (D. Minn. Dec. 14, 2001).

66 *Id.* at 1065.

67 *Bach*, 2001 U.S. Dist. LEXIS 21853, at *7. Because *Bach* involved state, not federal, officers, § 3105 did not strictly apply. The district court's reasoning is a bit opaque, and it is unclear whether the court held that violations of § 3105 violate the Constitution, or rather that such violations should be factored in as part of the court's weighing of the "reasonableness" of the search.

68 *Bach*, 310 F.3d at 1066.

69 *Id.* at 1067.

70 Of course, the defendant can still argue that the lack of officer presence made the search unreasonable, and thus violated the Fourth Amendment. *Cf.* United States v. Sparks, 265 F.3d 825, 830–32 (9th Cir. 2001) (discussing the reasonableness of using a private party–victim to conduct a search).

ment.[71] The factors listed by the court to support its holding that the search was reasonable highlight an inapposite comparison, "no warrant was physically 'served,' no persons or premises were searched in the traditional sense, and there was no confrontation between Yahoo! technicians and Bach."[72] Notice that each of these factors result directly from the fact that this "warrant" operates like a compulsory court order, not a search warrant.

By and large, these hybrid opinions have weakened the protections found in the three sources of positive law that make up the procedural net. The *Bach* reasoning is not premised on the fact that the "search" occurred in the electronic world nor on the fact that a compulsory subpoena-like process was used.[73] In other words, weak privacy protections for SCA warrants may lead to weak privacy protections for physical search warrants as well.

Aside from confusing court opinions, another problem is that whenever the strictures of search warrant procedural law collide with the practices of e-mail evidence gathering, prosecutors likely will react by asking Congress to amend the SCA to carve out exceptions from the procedural rules. "This rule from Rule 41 should not apply in the e-mail search context," the prosecutors will argue, "because the privacy interests are not the same." The result is a waste of executive and legislative branch time and energy and a patchwork SCA destined to become riddled with exceptions and exceptions to exceptions. For example, in the wake of the *Bach* litigation, the Department of Justice sought an amendment to § 2703, which Congress approved and the President signed into law. The new provision, § 2703(g), provides:

> Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.[74]

In other words, § 3105 does not apply to these warrants. This likely is not the last time that a federal statute or rule relating to search warrants will be found inconsistent with § 2703(a) warrants. One can imagine a patchwork collection of dozens of subsections just like 2703(g), each beginning, "Notwithstanding *some other federal rule* . . . ."

The results presaged above—confusing court opinions, wasted legislative energy, and patchworked exceptions to the rules—will become our reality unless we revise the statute to remove the fiction that these are warrants at all.

As a hypothetical example, consider the recently-added "nationwide service of process" rule for § 2703(a) warrants. Section 220 of the USA PATRIOT Act amended § 2703(a) to explicitly allow a court to issue a 2703(a) warrant to obtain e-mail messages even if the messages resided outside the

---

71 *Bach*, 310 F.3d at 1067.

72 *Id.*

73 *See id.* at 1067–68.

74 21st Century Department of Justice Appropriations Authorization Act, Pub. L. No. 107-273, § 11010, 116 Stat. 1762, 1822–23 (2002) (codified at 18 U.S.C.A. § 2703(g)).

court's physical jurisdiction, so long as the court had "jurisdiction over the offense."[75] Prior to this amendment, some courts had declined to issue 2703(a) warrants for e-mail messages outside their district because Rule 41 is limited to searches and seizures of "property . . . within the district."[76] This caused an enormous administrative burden on districts such as the Eastern District of Virginia and the Northern District of California that housed major ISPs.[77]

It is conceivable that magistrate judges, confused by the interplay between § 2703(a) and Rule 41(b), may someday errantly rule that SCA warrants do not have nationwide reach. To be clear, it is unambiguous from the text and legislative history that Congress specifically intended to create nationwide jurisdiction for courts with jurisdiction over the offense. Section 220 of the USA PATRIOT Act is entitled, "Nationwide Service of Search Warrants for Electronic Evidence."[78] The amendment changed the phrase "pursuant to a warrant issued under the Federal Rules of Criminal Procedure" to read, "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."[79] Furthermore, in the report of the House Judiciary Committee accompanying the USA PATRIOT Act, the committee explained:

> Title 18 U.S.C. § 2703(a) requires a search warrant to compel service providers to disclose unopened e-mails. This section *does not affect the requirement for a search warrant*, but rather attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet. Currently, Federal Rules of Criminal Procedure 41 requires that the "warrant" be obtained "within the district" where the property is located. An investigator, for example, located in Boston who is investigating a suspected terrorist in that city, might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California. The investigator would then need to coordinate with agents, prosecutors and judges in the district in California where the ISP is located to obtain a warrant to search. These time delays could be devastating to an investigation, especially where additional criminal or terrorist acts are planned.
>
> Section 108 amends § 2703 to authorize the court with jurisdiction over the investigation to issue the warrant directly, without requir-

---

75 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, § 220(a)(1), 115 Stat. 272, 291–92.

76 *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, FIELD GUIDANCE ON NEW AUTHORITIES THAT RELATE TO COMPUTER CRIME AND ELECTRONIC EVIDENCE ENACTED IN THE USA PATRIOT ACT OF 2001, http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last updated Nov. 5, 2001).

77 *Id.*

78 USA PATRIOT Act § 220, 115 Stat. at 291.

79 *See id.* § 220(a)(1).

> ing the intervention of its counterpart in the district where the ISP is located.[80]

Despite this legislative clarity, a court might errantly read the phrase, "using the procedures described in the Federal Rules of Criminal Procedure" to import Rule 41(b)(1)'s jurisdictional limitation to magistrate judges "within the district" where the property to be searched is located. Although this reading would be provably mistaken, it is another example of the confusion that can emerge when two procedural regimes are inartfully stuck to one another.

Furthermore, these are not the only situations where this confusion may arise. Anywhere the distinction between a "warrant" executed by officers and an "order" served on custodians is important, the distinction will matter.

If Congress were to relabel § 2703(a) warrants to be "probable cause orders," then it would need to clarify which procedural rules apply. One half-measure would be to keep the textual pointer to the Federal Rules of Criminal Procedure, although that solution seems to lead us right back to where we started. A better proposal would be for Congress to parse through Rule 41 and §§ 3101–3118, and to decide which provisions should apply to § 2703(a). It could then specify in the body of § 2703 exactly what a § 2703(a) order should look like.

The model can be § 2703(d). This section defines a type of court process that investigators may use to obtain certain types of content from ISPs, not including the type of unopened, unretrieved e-mail messages that trigger § 2703(a). Section 2703(d) is not tied in any way to Rule 41 nor any other federal procedural statutes. It provides:

> (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.[81]

Section 2703(d) orders are much less formally specified than Rule 41 search warrants. No description is given for the form in which the "specific and articulable facts" must be given. No mention is made for the time in which the order must be executed, or whether a report must be made to the issuing court.

---

80 H.R. REP. NO. 107-236, pt. 1, at 57 (2001).

81 18 U.S.C.A. § 2703(d) (West 2003).

Which procedures is Congress likely to deem necessary to § 2703(a)? Of course, the substantive standard should remain "probable cause." Secondly, the new provision should retain Rule 41(c)'s limitation that search warrants can only be used to search for "(1) evidence of a crime; (2) contraband, fruits of a crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime."[82] Furthermore, Congress is likely to authorize a "motion to quash" on the part of ISP as it has with § 2703(d) orders. There may be others, of course, but the new provision, in redline form, could read:

> (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 an ~~warrant~~ order 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. This court order shall issue only if there is probable cause to obtain property under Federal Rule of Criminal Procedure 41(c). 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. 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.

The new provision is longer, but no less easy to understand. It proves, once again, the age-old maxim (which I just made up) that "there are no elegant amendments to the Electronic Communications Privacy Act."[83]

IV. Conclusion

I have intended to list strategies that increase accountability and awareness about the state of privacy and security in our surveillance laws. These are not the only such changes that could be made to the Internet surveillance statutes. Other possible changes include additional reporting requirements, changes to provisions governing notice to users whose communications have been obtained, and increased judicial oversight. I am heartened to see that

---

82 FED. R. CRIM. P. 41(c). The fourth subcategory of the list, "a person to be arrested or a person who is unlawfully restrained," FED. R. CRIM. P. 41(c)(4), does not apply to searches for electronic communications and thus is not included in this list.

83 For additional proof, see Professor Kerr's sensible, ungainly proposed amendment in this very Symposium. Kerr, *supra* note 1, at 1235–37.

many of the recommendations made by the other participants in this Symposium have been of this nonsubstantive type, and I hope to see more of these recommendations in the future.