Washington University Global Studies Law Review

Volume 7 | Issue 1

January 2008

A Schrödinger's Onion Approach to the Problem of Secure Internet Communications

Joshua A. Altman
Washington University School of Law

A SCHRÖDINGER'S ONION APPROACH TO THE PROBLEM OF SECURE INTERNET COMMUNICATIONS

ABSTRACT

The laws governing privacy in electronic communications have developed as a statutory response to a problem of constitutional magnitude. Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA)[1] to extend constitutional norms to emerging contexts. Congress did so after the absence of such statutes caused confusion and uncertainty, obviated post hoc decision-making by the courts, and chilled rights. The age of the Internet has transformed our social conditions respecting the freedoms of speech and privacy, as well as our public needs respecting security. But the ECPA has not been amended to be Internet regarding. Those modifications which have been implemented have been in response to changes in politics and not to changes in technology.

Emerging technologies highlight the failures of our present statutory scheme. One such technology, the Tor network, employs onion routing to enable anonymous Internet communication at the socket level. Anonymity as such frustrates the extension of property law into the privacy context. Privacy doctrine derived from the law of real property fills our case- and codebooks and chills our actions by retrofitting previously inconceivable modes of communication into ancient analogies. Further, these technologies themselves have both the power to legislate human activity as well as dictate statutory and constitutional capabilities.

Understanding that technology will present us with ever more complex issues, we require new, creative solutions to animate old constitutional principles. Much of the debate has focused on institutional competence to adapt to a changed landscape. I propose that, before we reach the question of institutional competence, we decide some basic presumptions. I advocate a baseline shift in the form of a Schrödinger's Onion approach. In the absence of knowledge, we should presume the object of our inquiry demands the highest protection.

U.S. citizens engaged in lawful acts are entitled to heightened protection against their constitutional rights' deprivation by surveillance or disclosure of their electronic communications or records to governmental

1. 18 U.S.C. §§ 2510–2521, 2701–2711, 3121–3127 (2006).

entities. The reach of those fundamental rights has been limited to statutory protection when information is electronically transmitted to a third party. The review afforded non-citizens engaged in the same transactions is still uncertain. Determining to whom Internet packets and records relate—whether they relate to U.S. citizens and are thus entitled to a high standard of scrutiny for subpoena or they relate to non-citizens and thus could require something less—invites a Schrödinger's Onion approach: without examining the unencrypted packets in full, one must presume they relate at once to both U.S. citizens and non-citizens alike.

TABLE OF CONTENTS

INTRODUCTION

In the Internet, we now have a complex network of copper and fiber-optic lines, vast trunks and massive satellite and radio transponders, linking, by integrated switches and duplicative, distributed routers, servers of information in virtually every corner of the earth, and a few extra-terrestrial locations.[2] The Internet is a medium; it facilitates many protocols of transmission.

The Tor network enables individuals to access sites and services available on the Internet in ways that are, at once, secure and anonymous. It does so by employing a decentralized network of servers located throughout the world. To use the Tor network, individuals operate Tor clients, which cipher and decipher information, to make use of Tor servers, which relay information from a point of entry, to other Tor servers, to a point of exit and on to publicly accessible Internet locations. When a user transmits and receives information vis-à-vis the Tor network, that information is both encrypted and encapsulated: encryption hides the user's content; encapsulation hides the user's identity.

To illustrate the difficulties such a network imposes on current privacy law, I advance the following hypothetical scenario. A woman in Kadiköy receives a text message on her cellular phone from an associate. She enters an Internet café, pays a nominal fee, sits at a terminal and nervously executes a small program residing on a USB drive. Traffic from her computer travels through Dresden, then through Jacksonville, Panama City, Tokyo, back across the Pacific Ocean, and, upon re-entering the public routing network through a server in Portland, establishes a secure tunnel with a server in St. Louis. After several minutes, the woman leaves, her communication complete.

Meanwhile, a local police department in Portland continues an investigation in the wake of a recent murder. After obtaining a warrant to access the victim's computer and then looking through the victim's e-mail, Detective Copal discovers a suspicious message sent from an anonymous

2. Besides the obvious use of satellites in Internet communications, there are numerous projects currently aimed at interplanetary Internet broadcasts. *See About—Delay Tolerant Networking Research Group*, http://www.dtnrg.org/wiki/About (last visited Oct. 18, 2007). Recently, the Mars rover, Spirit, "sent a transmission to the European Space Agency's Mars Express, an orbiting craft, which then transmitted the data to Earth." Joanna Glasner, *Wired News: Pushing the Internet Into Space*, http://www.wired.com/news/technology/0,70377-0.html (last visited Oct. 18, 2007). The Messenger probe to Mercury recently used the Coherent File Distribution Protocol (CFDP), which "allows an instrument to record an observation in a file and transmit the file to Earth without having to consider whether physical transmission is possible at that time. . . ." *Id.*

account. Trying to determine the source of the message, Detective Copal can identify the source IP as a Tor exit point. The Detective would like to obtain log files from the Tor server in Portland.

In a federal office building in Denver, an agent continues his investigation into a child pornography operation in Frisco, Colorado. Reading public message boards, Agent Fabian finds that a user with an IP address traceable to Portland has posted links to several foreign web sites operated by the child pornography ring. Agent Fabian has determined that the IP address belongs, in fact, to a Tor exit point. Agent Fabian would like to monitor communications and obtain log files from the Tor server in Portland.

In another federal office building in Fort Meade, Maryland, an agent continues her diligent pursuit of terrorist activity. Agent Nasal monitors all Internet traffic arriving in the United States from Japan. She keeps a list of suspicious IP addresses, and includes those running Tor servers. At the precise atomic time that Agent Nasal expects a transmission, a connection is made between Tor servers in Tokyo and in Portland. Agent Nasal has a list of servers that communicated with each server before and after that transmission, but does not know the content of the packets in question, where they came from or where they went to. Agent Nasal would like to monitor future communications and obtain archival log files from the Tor server in Portland.

Three hours later, the woman in Kadiköy returns to the Internet café. Again, she re-routes her traffic through the Tor network. She begins to cry tears of joy and leaves. She has learned that her husband has been granted asylum in the United States, and that she and her son will soon be joining him.

Each actor in our hypothetical has a compelling interest in reinforcing or piercing the veil of privacy. But current law fails to deal with the problem Tor creates. As you will see below, none of the governmental actors knows the object of his or her inquiry, or even to whom that object relates. This is problematic. Privacy doctrine is largely based on concepts derived from the law of real property. Further, the Fourth Amendment has been increasingly subject to codification. In this arena, constitutional principles are, essentially, animated only insofar as Congress has had the foresight to specify. In the 1960s and again in the 1980s, Congress introduced laws that incrementally modernized privacy law to account for changes in technology and social conditions. Though these variables have again transformed our landscape, there have not been such changes made in the age of the Internet. Those changes which have been implemented

have been in response to changes in politics and not to changes in technology.

In light of the difficulties inherent in reconciling contrary and equally seductive policies in light of brave new technologies, we must again rethink our privacy doctrine. This requires distilling new and creative solutions to the problems emerging technologies introduce.

Much of the debate has focused on the institutional competence of the various custodians of privacy law. Strong arguments exist that Congress, ad hoc, is best able to ensure that law keeps pace with technology, and thus that the codification of the Fourth Amendment is a good thing. Alternatively, the courts, post hoc, are geared to animate constitutional norms by entertaining challenges based on the source of those principles when faced with actual controversies. Another approach understands technologists to be capable of regulating the capacities of their wares. A corollary is that the technologies themselves are capable of evading regulation.

In this Note, I argue that there is a preliminary question that must be answered: what do we do in the absence of knowledge? I contend the answer lies in the classic Schrödinger's Cat scenario.[3] Having only enough information to know the stakes involved, we must presume the cat is, at once, alive and dead. If we value the cat's life, we must hesitate before opening the box. Similarly, in a Schrödinger's Onion approach, if we value privacy, we must presume the object of our inquiry deserves the highest protection.

In the first section, this Note provides a brief introduction to and history of the Internet before examining the intricacies and implications of the Tor network.[4] In the second section, this Note explores the development of privacy law in the United States, fleshing out the various

---

3. In the Schrödinger's Cat scenario,

> A cat is penned up in a steel chamber, along with . . . a tiny bit of radioactive substance, *so* small that *perhaps* in the course of one hour one of the atoms decays . . . releas[ing] a hammer which shatters a small flask of hydrocyanic acid . . . . [O]ne would say that the cat still lives *if* meanwhile no atom has decayed. The first atomic decay would have poisoned it. The [psi] function for the entire system would express this by having in it the living and the dead cat (pardon the expression) mixed or smeared out in equal parts.

Erwin Schrödinger, *Die gegenwärtige Situation in der Quantenmechanik*, 23 Naturwissenschaften 807–12, 823–28, 844–49 (1935), *translated in* John D. Trimmer, 124 *Proceedings of the American Philosophical Society* 323, 328 (1980).

4. This Note provides an extremely abridged overview of electronic privacy law, as this topic has received extensive treatment elsewhere. For a more detailed description, see U.S. DEP'T OF JUSTICE OFFICE OF LEGAL EDUC., PROSECUTING COMPUTER CRIMES (Scott Eltringham ed., 2007) and U.S. DEP'T OF JUSTICE COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002).

constitutional principles and statutory schemes currently regulating government entities' access to electronic communications and records. Finally, in the third section, this Note proposes a way to begin a conversation about privacy doctrine in the age of the Internet, with an eye to the Constitution's nobility.

I. THE PROBLEM TOR CREATES

In 1970, the University of Brussels hosted an International Colloquium on the European Convention[5] and privacy rights. In an address to the Colloquium, University of Aberdeen Professor R.V. Jones observed:

> Attempts at the penetration of privacy have probably occurred in all conscious societies from before classical times, but their scope was until recently restricted by the limitations on the propagation of light and sound from the individual under surveillance to a hidden observer or eavesdropper. The invention of the telescope and of photography began to broaden the limits of observation, and these were widened further by the microphone and telephone; but the event that led to the modern explosion of surveillance techniques was the discovery of the electron in 1897 by J.J. Thomson. In fact, we in this colloquium may well sympathise with the toast that is said to have been drunk by the research workers in Thomson's laboratory, the Cavendish, at one of their annual dinners: "To the electron—may it never be of any use to anybody!"[6]

Alas, the electron has survived. We now live in the age of the Internet.

A. The Internet, Briefly

The Internet was sparked by a desire for a communications system that would survive a nuclear attack. In August 1962, working at the Massachusetts Institute of Technology and at Bolt Beranek and Newman, Inc., J.C.R. Licklider[7] wrote a series of memoranda in which he imagined

5. The European Convention on Human Rights was signed in Rome on November 4, 1950. Council of Europe—ETS no. 005— Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf.

6. R.V. Jones, *Some Threats of Technology to Privacy*, *in* PRIVACY AND HUMAN RIGHTS 139, 140 (A.H. Robertson ed., 1973).

7. Of special interest to this publication, the *Washington University Global Studies Law Review*, J.C.R. Licklider received bachelors of arts degrees in physics, math and psychology from Washington University in St. Louis in 1937, and a masters degree in psychology from the same institution in 1938.

a "galactic network."[8] In August 1964, working at the Rand Corporation, Paul Baran released a series of publications on distributed communications networks.[9] In the publications, Baran described "heuristic routing doctrines" that would enable data to traverse unique paths through decimated communications networks.[10]

The Defense Advanced Research Projects Agency (DARPA) "was established in 1958 as the first U.S. response to the Soviet launching of Sputnik."[11] Licklider was the first head of the computer research program at DARPA.[12] On November 21, 1969, Advanced Research Projects Agency Network (ARPANET) first linked computers at the University of California at Los Angeles and Stanford Research Institute.[13] In December 1969, computers at the University of Utah and the University of California at Santa Barbara were added to the network.[14] There were thirteen computers on the network "in January 1971, twenty-three in April 1972, sixty-two in June 1974 and 111 by March 1977."[15]

In May 1974, Robert E. Kahn, working at DARPA, and Vinton G. Cerf, working at Stanford University, developed a new Transmission Control Protocol (TCP) from the original ARPANET Network Control Protocol (NCP).[16] They proposed "that a computer sending messages should first enclose them in uniquely addressed digital 'envelopes,' also called datagrams, and send them to the gateway computer to be handed off

---

He received his doctorate in psychoacoustics from the University of Rochester in 1942. *J.C.R. Licklider*, http://en.wikipedia.org/w/index.php?title=J._C._R._Licklider&oldid=156239912 (last visited Sept. 11, 2007).

8. J.C.R. Licklider and W. Clark, *On-Line Man Computer Communication*, August 1962. *See, e.g.*, M. MITCHELL WALDROP, THE DREAM MACHINE: J.C.R. LICKLIDER AND THE REVOLUTION THAT MADE COMPUTING PERSONAL (Viking 2001).

9. Paul Baran, *On Distributed Communications: Introduction to Distributed Communications Network*, Rand Corp. Memorandum (RM-3420-PR, August 1964), http://www.rand.org/publications/RM/RM3420/; Paul Baran, *On Distributed Communications: V. History, Alternative Approaches, and Comparisons*, Rand Corp. Memorandum (RM-3097-PR, August 1964), http://www.rand.org/publications/RM/RM3097/.

10. "Baran envisaged a computer communications network that lacked a central authority and used 'heuristic routing doctrines' that could successfully transmit data over a heavily damaged infrastructure." Joseph B. Fazio, *Sputnik and its aftermath—Nuclear first-strike concerns—Distributed-network theory*, 1 INTERNET LAW and PRACTICE § 1:5.

11. DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, DARPA OVER THE YEARS (Oct. 27, 2003), http://www.darpa.mil/body/overtheyears.html.

12. Barry M. Leiner et al., *A Brief History of the Internet*, http://www.isoc.org/internet/history/brief.shtml (last visited Sept. 11, 2007).

13. MARTIN DODGE AND ROB KITCHIN, MAPPING CYBERSPACE 7 (Routledge 2001).

14. *Id*.

15. *Id*.

16. Vinton G. Cerf and Robert E. Kahn, *A Protocol for Packet Network Intercommunication*, COM-22 IEEE TRANS. on COMM. 637, 637–48 (May 1974).

to other networks."[17] In 1978, TCP was split in two, separating the Internet Protocol (IP) to be exclusively used for routing information; and, in 1983, NCP was completely replaced by TCP/IP.[18]

As presently constructed, the Internet operates by routing such encapsulated IP packets from network to network. Each "host in the Internet is identified by a globally unique IP address" and the "IP Packet header[s] contains an IP network address for the sender and an IP network address for the destination."[19] Each router "must determine the next hop in the route to the destination and then encapsulate the IP packet into the frame of the type of the next network or link."[20]

B. Onion Routing and the Tor Network

Internet communications are most transparent when the IP packet headers contain the actual sender's and actual recipient's or destination's IP network addresses, and the unencapsulated packets themselves contain plaintext. However, such transparent communication presents privacy problems akin to the party line telephone. The Naval Research Laboratory's Center for High Assurance Computer Systems recognized these problems:

> Letters sent through the Post Office are usually in an envelope marked with the sender's and recipient's addresses. We trust that the Post Office does not peek inside the envelope, because we consider the contents private. We also trust that the Post Office does not monitor who sends mail to whom, because that information is also considered private.
>
> These two types of sensitive information, the contents of an envelope and its address, apply equally well to electronic communication over the Internet and the Web. As the Web becomes an important part of modern day communication and electronic commerce, protecting the privacy of electronic messages becomes

17. ENCYCLOPEDIA OF NEW MEDIA: AN ESSENTIAL REFERENCE TO COMMUNICATION AND TECHNOLOGY 68 (Steve Jones ed., Sage Publications Ltd. 2003).

18. *Id*. Today, the "TCP/IP protocol suite usually refers not only to . . . the *Transmission Control Protocol (TCP)* and the *Internet Protocol (IP)* but also to other related protocols such as the *User Datagram Protocol (UDP)*, the *Internet Control Message Protocol (ICMP)* and the basic applications such as HTTP, TELNET, and FTP." ALBERTO LEON-GARCIA AND INDRA WIDJAJA, COMMUNICATION NETWORKS: FUNDAMENTAL CONCEPTS AND KEY ARCHITECTURES 573 (McGraw-Hill Professional 2004).

19. *Id*. at 574–75.

20. *Id*. at 575.

> increasingly important. Just like mail, electronic messages travel in electronic envelopes. Protecting the privacy of electronic messages requires both safeguarding the contents of their envelopes and hiding the addresses on their envelopes. Although communicating parties usually identify themselves to one another, there is no reason that the use of a public network like the Internet ought to reveal to others who is talking to whom and what they are talking about. The first concern is traffic analysis, the latter is eavesdropping.[21]

In 1995, the Office of Naval Research[22] began work on an onion routing system and, in 1997, was joined by DARPA.[23] In 2004, the EFF[24] continued funding for the project.[25]

An onion routing network is unique, because the actual sender's IP network address is encrypted inside the encapsulated packet.

---

21. David M. Goldschlag, Michael G. Reed, and Paul F. Syverson, *Privacy on the Internet*, Apr. 17, 1997, http://www.onion-router.net/Publications/INET-1997.html.

22. Established in 1946, the Office of Naval Research's Mission is "[t]o Foster, plan, facilitate and transition scientific research in recognition of its paramount importance to enable future naval power and the preservation of national security." *History and Mission of ONR*, http://www.onr.navy.mil/about/history/ (last visited Sept. 11, 2007).

23. DARPA was founded in 1958. *DARPA Over the Years*, http://www.darpa.mil/body/overtheyears.html (last visited Sept. 11, 2007). DARPA's statutory authority authorizes it to engage in research programs towards the "exploitation of opportunities that hold the potential for yielding significant military benefits." 10 U.S.C. § 2352(b)(2)(B) (2006). The original Department of Defense directive, 5105.15, gave DARPA responsibility "for the direction or performance of such advanced projects in the field of research and development as the Secretary of Defense shall, from time to time, designate by individual project or by category." *ARPA/DARPA*, Apr. 14, 2006, http://www.darpa.mil/body/arpa_darpa.html.

In 1958, DARPA was originally called the Advanced Research Projects Agency (ARPA); in 1972, the name was changed to DARPA; in 1993, the name was changed back to ARPA; and, in 1996, the name was changed again to DARPA. *Id.* Throughout this Note, the Agency is referred to as DARPA.

24. The EFF, founded in 1990 by the founder of Lotus Development Corp., Mitch Kapor, is a non-profit organization whose mission is to:

> 1. Engage in and support educational activities which increase popular understanding of the opportunities and challenges posed by developments in computing and telecommunications.
>
> 2. Develop among policy-makers a better understanding of the issues underlying free and open telecommunications, and support the creation of legal and structural approaches which will ease the assimilation of these new technologies by society.
>
> 3. Raise public awareness about civil liberties issues arising from the rapid advancement in the area of new computer-based communications media. Support litigation in the public interest to preserve, protect, and extend First Amendment rights within the realm of computing and telecommunications technology.
>
> 4. Encourage and support the development of new tools which will endow non-technical users with full and easy access to computer-based telecommunications.

EFF: Formation documents and mission statement for the EFF (July 10, 1990), http://www.eff.org/legal/cases/SJG/?f=eff_creation.html.

25. *Onion Routing: Brief Selected History*, http://www.onion-router.net/History.html (last visited Sept. 11, 2007).

> Before sending data over an anonymous connection, the first Onion Router adds a layer of encryption for each Onion Router in the route. As data moves through the anonymous connection, each Onion Router removes one layer of encryption, so it finally arrives as plaintext. This layering occurs in the reverse order for data moving back to the initiator.[26]

Additionally, the content of the unencapsulated packet is further encrypted on a layer beneath that of the IP packet headers. This layered approach to IP packets resembles an onion.

In the Tor network, a decentralized system of servers around the world, such uniquely encrypted packets pass from an end user, along a chain of servers, and to a destination host, and back again. In most cases, the Tor servers do not maintain logs of source and destination Internet Protocol addresses.[27] As all packets traveling across the Tor network are encrypted, the content of the information is unobtainable by any entity attempting to intercept it. Similarly, routing information is unavailable to any entity attempting to identify the source and destination of these packets. A user, accessing this network over a client program on his or her computer, is thus able to access any website in the world from anywhere in the world, in virtual anonymity.

Internet users employ the Tor network, and other anonymizing protocols,[28] for a variety of reasons and in a variety of contexts. The Tor

---

26. Generally,

> Onion Routing works in the following way: An application, instead of making a (socket) connection directly to a destination machine, makes a socket connection to an Onion Routing Proxy. That Onion Routing Proxy builds an anonymous connection through several other Onion Routers to the destination. Each Onion Router can only identify adjacent Onion Routers along the route. Before sending data over an anonymous connection, the first Onion Router adds a layer of encryption for each Onion Router in the route. As data moves through the anonymous connection, each Onion Router removes one layer of encryption, so it finally arrives as plaintext. This layering occurs in the reverse order for data moving back to the initiator. Data passed along the anonymous connection appears different at each Onion Router, so data cannot be tracked en route and compromised Onion Routers cannot cooperate. When the connection is broken, all information about the connection is cleared at each Onion Router.

Onion Routing: Executive Summary, http://www.onion-router.net/Summary.html (last visited Oct. 18, 2007).

27. *TheOnionRouter/TorFAQ*, http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ (last visited Oct. 18, 2007).

28. In addition to the Tor network, other anonymizing protocols exist. For examples of other anonymous internet surfing technologies, see *Remailers* (2005), http://www.emailprivacy.info/remailers. *See also Anonymizer—Internet Privacy & Security Solutions* (2007), http://www.anonymizer.com; *JAP—Anonymity & Privacy* (2006), http://anon.inf.tu-dresden.de/index_en.html.

network has been used by casual web surfers, business users, journalists, human rights workers and the United States Navy.[29]

C. Tor's Implications

Governmental entities must obtain a warrant, administrative subpoena, or court order to lawfully intercept communications or to seize records belonging to domestic citizens. Warrants and court orders require probable cause. Administrative subpoenas require an authorized investigation to protect against enumerated threats and must not be aimed solely at First Amendment activities. However, because it is impossible for the governmental entities to know the communications' parties or the records' owners, all communications in the Tor network must be presumed to belong to domestic citizens in order to ensure that citizens' rights are not violated.

Congress' power to invade the privacy rights of non-citizens may be plenary. This governmental presumption is evidenced by FISA provisions allowing for searches without probable cause, as well as by the USA PATRIOT Act and Protect America Act's modifications to FISA and the ECPA. The Tor network, however, presents an arena wherein this power must be checked. Evidence of a reasonable expectation of privacy in secure communication invokes the requirements of Due Process in the interest of citizens' First, Fourth, Fifth, and Fourteenth Amendment rights. Although governmental entities have legitimate security concerns,[30] to sufficiently protect the relevant constitutional rights, the protections of the Fourth Amendment Title III, and ECPA must be extended to all electronic communications.

Finally, the technology itself disables governmental entities' interception of the communications and access to the records. From all indications, it is clear that both encryption and onion routing will continue to improve. The technological impossibility of governmental entities intercepting the communications and accessing the records serves to

29. *Tor: Overview* (Jan. 25, 2007), http://tor.eff.org/overview.html.en. For an interesting analysis of the use of the Tor network, as well as simple proxy servers, to get around China's "great firewall," see Tom Zeller Jr., *The Basics: How to Outwit the World's Internet Censors*, N.Y. TIMES, Jan. 29, 2006, at Section 4.

30. The National Security Estimate on global terrorism and Iraq was recently declassified. Of note: "The radicalization process is occurring more quickly, more widely, and more anonymously in the Internet age, raising the likelihood of surprise attacks by unknown groups whose members and supporters may be difficult to pinpoint." *Declassified Key Judgments of the National Intelligence Estimate on Global Terrorism*, N.Y. TIMES, Sept. 27, 2006, at Section A.

highlight the necessity of third party compliance. Law must keep up with technology by respecting and ensuring emerging privacy interests. This would legitimize governmental surveillance and requests for records and, coordinately, increase the likelihood of cooperation.

II. HOW THE LAW DOES NOT RESPOND

A. The Constitution

"There is no explicit right to privacy in the United States Constitution. The Supreme Court has ruled that there is a limited constitutional right of privacy based on several provisions in the Bill of Rights."[31] A number of amendments to the United States Constitution have been held to establish a right to privacy. That is, "[v]arious guarantees create zones of privacy."[32] For example, First Amendment jurisprudence respecting the right to privacy relies on the right to anonymous speech,[33] as well as the "vital relationship between freedom to associate and privacy in one's associations."[34]

Different privacy interests are supported by different constitutional provisions. Just as there is neither an explicit constitutional right to privacy nor a general privacy statute, electronic records held by third

---

31. ELECTRONIC PRIVACY INFORMATION CENTER, PRIVACY & HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND DEVELOPMENTS 708 (2004).

32. Griswold v. Conn., 381 U.S. 479, 484 (1965).

> The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."
>
> The Fourth and Fifth Amendments were described in *Boyd v. United States*, 116 U.S. 616, 630 [1886], as protection against all governmental invasions "of the sanctity of a man's home and the privacies of life." We recently referred in *Mapp v. Ohio*, 367 U.S. 643, 656 [1961], to the Fourth Amendment as creating a "right to privacy, no less important than any other right carefully and particularly reserved to the people."

Id. at 484–85.

33. In *Watchtower Bible & Tract Soc'y of N.Y. v. Village of Stratton*, 536 U.S. 150, 153, 162 (2002), finding a right to "anonymous political speech" en route to declaring unconstitutional a registration requirement for door-to-door canvassers, the Court found Jehovah's Witnesses' canvasses to be high value speech "as vehicles for the dissemination of ideas."

34. Nat'l Ass'n for Advancement of Colored People v. State of Ala. *ex rel*. Patterson, 357 U.S. 449, 462 (1958).

parties require specific statutory protection.[35] With respect to Constitutional principles, this Note focuses on the penumbral right to privacy, which extends from the Fourth Amendment, and the corresponding Due Process guarantees of the Fifth and Fourteenth Amendments,[36] which check and inform the statutory regulations.

1. The Fourth Amendment

There were two approaches to early Fourth Amendment[37] jurisprudence. One approach equated unlawful requests for information with unlawful search and seizure.[38] The other approach required physical trespass on "protected areas."[39] Such physical trespass on protected areas evolved into "an intrusion into a zone of privacy,"[40] with a number of

35. ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 31, at 708. "Rather than enact general statutory protections for personal data, the United States has taken a sectoral approach to privacy regulation so that records held by third parties, such as consumer marketing profiles or telephone calling records, are generally not protected unless a legislature has enacted a specific law." *Id.*

36. As this Note focuses on the differences in the protections afforded to citizens and non-citizens, it is worth noting that the Due Process Clauses of the Fifth and Fourteenth Amendments make no reference to citizenship; the same protections are afforded to all persons. U.S. CONST. amend. V ("nor shall any person . . . be deprived of life, liberty, or property, without due process of law"); U.S. CONST. amend. XIV ("nor shall any State deprive any person of life, liberty, or property, without due process of law").

37. The Fourteenth Amendment provides:

> 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 searched.

U.S. CONST. amend. IV. For a discussion of the history of the Fourth Amendment, see Robert S. Steire, Note, *Keeping "Private E-mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 234–46 (1998).

38. *See Boyd*, 116 U.S. at 630.

39. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928); Hester v. United States, 265 U.S. 57, 59 (1924). Interestingly, in a famous dissent in *Olmstead*, cited by the Senate Judiciary Committee in its report on the ECPA, Justice Brandeis wrote:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . [sic] Can it be that the Constitution affords no protection against such invasions of individual security?

S. Rep. No. 99-541, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556 (citing *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting)).

40. United States v. Miller, 425 U.S. 435, 440 (1976). "'[N]o interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.'" *Id.* (quoting Hoffa v. United States, 385 U.S. 293, 301–02 (1966)).

important qualifiers.[41] *Katz v. United States*[42] established a test to determine whether the affected person had a reasonable expectation of privacy.[43] The reasonableness of such an expectation depends on how society understands[44] the nature of the invaded property.[45] "Fourth Amendment doctrine has remained heavily tied to real property concerns."[46]

The privacy interest one retains in information transmitted to a third party is unclear.[47] Where courts have found no reasonable expectation of privacy, they have highlighted factors evidencing consent.[48] More recently, courts have narrowed the inquiry and have found a reasonable

---

41. In *Miller*, the Court held that the

> Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. at 443. The qualifiers in this language suggest that the Fourth Amendment is not entirely inapplicable to information revealed to a third party; however, this case is generally cited to support the proposition that "individuals do not have constitutional privacy interests in data transferred to third parties, meaning that specific statutes would have to be enacted to protect data held by others." ELECTRONIC PRIVACY INFORMATION CENTER, *supra* note 31, at 708.

42. 389 U.S. 347 (1967).

43. *Id*. In *Katz*, the Court recognized that the "Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351 (internal citations omitted).

Since the decision in *Katz*, it has been the law "that capacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place." Rakas v. Illinois, 439 U.S. 128, 143 (1978).

44. "A subjective expectation of privacy is legitimate if it is one that society is prepared to recognize as reasonable." Minnesota v. Olson, 495 U.S. 91, 95–96 (1990) (internal quotations omitted).

45. *See, e.g.*, United States v. Ohnesorge, 60 M.J. 946, 948 (2005). "Whether a person has a Fourth Amendment reasonable expectation of privacy in communications from one's private computer depends upon the nature of the communication." *Id*.

46. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809 (Mar. 2004). Professor Kerr highlights the adoption in this context of concepts derived from the "right to exclude," the rules applicable to "closed containers," and those rules affecting a "meaningful interference with an individual's possessory interest." *Id.* at 810, 812, 814. For a comprehensive history of the development of current privacy law, see *id.* at 839–55.

47. *See supra* note 12.

48. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that there is no such expectation in the numbers dialed on a telephone because the telephone company was expected to access the information); United States v. Simons, 206 F.3d 392 (4th Cir. 2000) (holding that an employee did not have a legitimate expectation of privacy with regard to his employer's record of his Internet usage under the circumstances involved). Some argue that, *per se*, there may be no reasonable expectation of privacy in Internet communications by employees at workplaces. *See, e.g.*, Mitchell Waldman, Annotation, *Expectation of Privacy in Internet Communications*, 92 A.L.R.5th 15 § 7 (2001) (suggesting that any policy placing employees on notice defeats a reasonable expectation of privacy).

expectation of privacy where the identity of the parties and the content of the communication suggest the user's expectation should not be defeated.[49]

Berger v. New York[50] defined the procedural safeguards necessary to protect the privacy interest. Once a user establishes such a reasonable expectation of privacy, the inquiry shifts to whether the statute at issue sufficiently protects that right to privacy.

2. The Fifth and Fourteenth Amendments

"The purpose of the Due Process Clause is to limit the power of the legislature to authorize arbitrary deprivation of rights of individuals."[51] In a seminal due process case, *Mullane v. Central Hanover Bank & Trust Co.*,[52] the Supreme Court observed that, while

> [m]any controversies have raged about the cryptic and abstract words of the Due Process Clause, . . . there can be no doubt that at a minimum they require that deprivation of life, liberty or property by adjudication be preceded by notice and opportunity for hearing appropriate to the nature of the case.[53]

The Supreme Court has consistently held that, through reverse incorporation, the constitutionally mandated process is substantially the same for the Fifth and Fourteenth Amendments.[54]

The liberty interests protected under the Fifth Amendment have been interpreted broadly.[55] Courts have held the Fifth and Fourteenth

---

49. *See* United States v. Maxwell, 45 M.J. 406, 417 (1996) (holding that "the tenor and content of the e-mail conversations between appellant and his correspondent, 'Launchboy,' reveal a reasonable expectation that the conversations were private"); Warshak v. United States, 490 F.3d 455, 470–71 (6th Cir. 2007), *reh'g granted* (Oct. 9, 2007) (finding a reasonable expectation of privacy in e-mail communications after narrowing the inquiry to identify the party with whom information was shared or from whom information was shielded, and the precise information actually conveyed); United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007) (finding a student had a reasonable expectation of privacy in information he transmitted over the university's network insofar as there was no announced monitoring policy).

50. 388 U.S. 41 (1967).

51. RICHARD J. PIERCE, JR., ADMINISTRATIVE LAW TREATISE 596 (4th ed. 2002).

52. 339 U.S. 306 (1950).

53. *Id*. at 313.

54. *See* Twining v. State of New Jersey, 211 U.S. 78, 100–01 (1908) (holding that "the part of the Constitution then before the court was the Fifth Amendment. If any different meaning of the same words, as they are used in the 14th Amendment, can be conceived, none has yet appeared in judicial decision").

55. Bolling v. Sharpe, 347 U.S. 497, 500 (1954) ("Although the Court has not assumed to define 'liberty' with any great precision, that term is not confined to mere freedom from bodily restraint. Liberty under law extends to the full range of conduct which the individual is free to pursue, and it

Amendments safeguard against arbitrary deprivations of liberty, creating a "sphere of personal privacy."[56] This "zone of privacy" protects the individual's interest in disclosing personal matters.[57] While there is no explicit reference to the right of privacy in the Bill of Rights, "the Supreme Court has recognized that such a right is implicit within various amendments to the Constitution."[58]

Some scholars have argued that "[p]iercing [an internet user's] anonymity without notice or the opportunity to challenge subpoena violates our most basic notions of procedural due process."[59] This school of thought seems to have gained some traction in the courts.[60]

---

cannot be restricted except for a proper governmental objective.").

56. United States v. Hubbard, 650 F.2d 293, 305 (D.C. Cir. 1980). "The fourteenth amendment's protection against arbitrary or unjustifiable state deprivations of personal liberty also prevents encroachment upon a constitutionally recognized sphere of personal privacy. The Fifth Amendment's protection of liberty from federal intrusion upon this sphere can be no less comprehensive." *Id*. at 304–05.

57. "The 'zone of privacy' safeguarded by the Constitution embraces 'the individual interest in avoiding disclosure of personal matters and . . . the interest in independence in making certain kinds of important decisions.'" Doe v. U.S. Civil Serv. Comm'n, 483 F. Supp. 539, 566 (S.D.N.Y. 1980)(citing Whalen v. Roe, 429 U.S. 589, 599–600 (1977)).

58. Foe v. Vanderhoof, 389 F. Supp. 947, 951 (D. Colo. 1975).

> A fundamental right to privacy for individuals is not specifically provided for in the United States Constitution; however, the Supreme Court has recognized that such a right is implicit within various amendments to the Constitution: *i.e.*, the First Amendment, Stanley v. Georgia, 394 U.S. 557, 89 S. Ct. 1243, 22 L.Ed.2d 542 (1969); the Fourth and Fifth Amendments, Terry v. Ohio, 392 U.S. 1 . . . (1968); Katz v. United States, 389 U.S. 347 . . . (1967); the Ninth Amendment, Griswold v. Connecticut, 381 U.S. 479 . . . (1965) (Goldberg, J., concurring); the penumbra of the Bill of Rights, *Griswold*, *supra* [note 32]; or in the concept of personal liberty guaranteed by the Fourteenth Amendment, *e.g.*, Meyer v. Nebraska, 262 U.S. 390 . . . (1923).

Id.

59. Shaun B. Spencer, *Cyberslapp Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace*, 19 JOHN MARSHALL J. OF COMPUTER & INFO. L. 493, 509 (2001) (citations omitted). Professor Spencer continues,

> [t]he core of due process is the right to notice and a meaningful opportunity to be heard. The Fifth and Fourteenth Amendments prohibit government from depriving citizens of life, liberty or property without due process of law. The exercise of First Amendment rights constitutes a protected liberty interest that the government may not deny without due process. Courts in a variety of contexts have held that judicial orders enforcing discovery requests constitute state action.

Id. at 509–10 (quoting LaChance v. Erickson, 552 U.S. 262, 266 (1998)).

60. *See infra* notes 113, 120 and 121 (discussing the U.S. District Court for the Southern District of New York's impact on and subsequent holding respecting the USA PATRIOT Improvement and Reauthorization Act of 2005).

B. The Statutes

Despite a public disagreement about its propriety,[61] Professors Kerr and Solove agree that, in the modern era, "statutory protections rather than constitutional protections provide the driving force behind wiretapping law."[62] Fourth Amendment jurisprudence affords greater constitutional protection against the contemporaneous interception of electronic communications than against the latent acquisition of stored communications. As such, governmental entities must satisfy a different standard when seeking to intercept communications in transmission, which is arguably constitutionally proscribed, than when seeking to access communications in electronic storage, which is statutorily proscribed.

1. Intercepted Communications

a. Omnibus Crime Control and Safe Streets Act of 1968

In 1968, Congress passed the Omnibus Crime Control and Safe Streets Act (Title III).[63] Title III prohibited the intentional interception,[64] use, or

---

61. *See* text Part III.

62. *See* Kerr, *supra* note 46. To this observation, Professor Solove adds: "We are witnessing a codification of the Fourth Amendment." Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 747 (2005).

63. 18 U.S.C. §§ 2510–2522 (2006). In its findings, Congress noted that "[t]here ha[d] been extensive wiretapping carried on without legal sanctions," and that "to protect effectively the privacy of wire and oral communications [and] . . . the integrity of court and administrative proceedings" and to "safeguard the privacy of innocent persons," "interception . . . should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court." Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 801, 82 Stat. 197, 211.

64. "Intercept" is presently defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). In the original text of Title III, intercept was defined as "the aural acquisition of the contents of any wire or oral communication through the use of any electronic, mechanical or other device." Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 212.

There is a fundamental ambiguity in the use of the word "acquisition." One court, concluding that "an 'acquisition' occurs at the time the recording is made," recognized that "an 'aural acquisition' could be said to occur whenever someone physically hears the contents of a communication" or that "a court facing the issue might conclude that an 'aural acquisition' is accomplished only when two steps are completed-the initial acquisition by the device and the hearing of the communication by the person or persons responsible for the recording." United States v. Turk, 526 F.2d 654, 657–58 (5th Cir. 1976).

For an interesting discussion of a circuit split that existed before the passage of the PATRIOT Act, see *infra* note 102. *See also* U.S. DEP'T OF JUSTICE OFFICE OF LEGAL EDUC., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002) (describing the Ninth Circuit's holding in United States v. Smith, 155 F.3d 1051, 1058–59 (9th Cir. 1998), which held that a party can intercept a wire communication by obtaining a copy of the

disclosure of oral[65] and wire[66] communications.[67] Title III mandated judicial oversight of wiretaps,[68] required probable cause for, and limited the circumstances under which judicial authorization for such interceptions could be obtained.[69] Title III included limited exceptions to this blanket prohibition[70] and expressly provided for the suppression of some evidence obtained in violation of provisions.[71]

b. Electronic Communications Privacy Act of 1986

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA).[72] In its findings, Congress recognized that "the law must advance

---

communication in electronic storage as, prior to the PATRIOT Act's passage, the definition of wire communication in 18 U.S.C. § 2510(1) specifically included "any electronic storage of such communication").

65. "Oral communication" is presently defined as "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." 18 U.S.C. § 2510(2).

66. "Wire communication" is presently defined as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (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.

Id. § 2510(1).

67. 18 U.S.C. § 2511(1). Analyzing the legislative history of the 1986 amendment to Title III, the Fourth Circuit summarized: "Voice communications transmitted via common carrier were protected under the 1968 act, but 'there [were] no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology.'" United States v. Suarez, 906 F.2d 977, 980 (4th Cir. 1990) (quoting S. REP. NO. 99-541, at 5 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559).

68. 18 U.S.C. § 2518.

69. *Id.* § 2516 (requiring, among other things, that a senior official in the Department of Justice show probable cause to believe the interception will reveal evidence of the commission of one of the enumerated felony offenses).

70. For a list of exceptions to the prohibition against interceptions, see 18 U.S.C. § 2511(2)(a)-(2)(h). Generally, the exceptions which permit warrantless governmental interception include: interception of radio transmissions; interception where the government is a party, has obtained prior consent from a party or where the fruits of an interception are disclosed by a service provider in limited circumstances; interception pursuant to the Foreign Intelligence Surveillance Act; interception where the transmission is readily accessible to the general public; interception with the use of a pen register or a trap and trace device; and interception of the communications of a computer trespasser in the course of an ongoing criminal investigation. *Id.*

71. *See* 18 U.S.C. § 2515. It is worth noting that only the fruits of unauthorized interceptions of oral and wire communications are suppressible. *Id.* While civil remedies are available for the unauthorized interception of electronic communications, no suppression remedy exists.

72. 18 U.S.C. §§ 2510–2521, 2701–2711, 3121–3127 (2006). Of note, the ECPA modified Title III to bring electronic communications within its purview. The other parts of the ECPA are

with the technology to ensure the continued vitality of the fourth amendment."[73] ECPA amended Title III to bring "'electronic communications' into general parallel with the 'wire' and 'oral' communications already subject to Title III protection against unauthorized interception, disclosure, or use."[74] However, Congress did not provide for the suppression of evidence obtained through the unauthorized interception of electronic communications.[75]

c. Foreign Intelligence Surveillance Act

In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA).[76] Under FISA, the Attorney General may authorize surveillance without a court order and, thus, without probable cause to believe that the target is a foreign power, for up to one year by certifying that the communication is between or among foreign powers.[77] Where the Attorney General seeks surveillance of a "United States person," a court

---

independently known as the Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2711 (2006), and the Pen/Trap Statute (Pen Register Act), 18 U.S.C. §§ 3121–3127 (2006). The SCA and Pen Register Act are examined below.

73. S. REP. NO. 99-541, at 5 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3559. The Senate Judiciary Committee continued: "Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right." *Id*.

74. Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995). Electronic communications are presently defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce. . . ." Specifically excluded from the definition are: "any wire or oral communication; any communication made through a tone-only paging device; any communication from a tracking device . . . [and] electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds." 18 U.S.C. § 2510(12) (2006).

75. *See* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (holding that the exclusivity provisions of the ECPA, at 18 U.S.C. § 2708, show that "Congress clearly intended for suppression not to be an option for a defendant whose electronic communications have been intercepted in violation of the ECPA"), *aff'd*, 106 Fed. App'x 688 (10th Cir. 2004); United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) ("The ECPA does not provide an independent statutory remedy of suppression for interceptions of electronic communications.").

76. Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1801 (2006).

77. *Id*. § 1802(a)(1).

> Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that the electronic surveillance is solely directed at the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers.

Id.

order is required.[78] The FISA court may only issue such a court order with probable cause to believe that the target is a foreign power.[79]

The Attorney General must then submit an application to the FISA court for certification.[80] The application must include a statement of the reasons for and the methods of the surveillance, and certification that the information sought pertains to foreign intelligence and that no other means of obtaining it exist.[81]

In August 2007, the Protect America Act, providing for sweeping changes to FISA, passed both chambers of Congress and was signed into law.[82] As of the date of this writing, it is unclear what impact the Act will have upon the interception of foreign communications. Most notably, the Act amended FISA to exclude from its definitions surveillance directed at persons reasonably believed to be located outside the United States, and empowered the Director of National Intelligence and the Attorney General to authorize certain acquisitions for up to one year with limited oversight.[83]

2. Stored Communications

a. The Electronic Communications Privacy Act of 1986

The ECPA created protections for stored electronic records of communications and customer information. Where the content of the

---

78. United States v. Squillacote, 221 F.3d 542, 553 (4th Cir. 2000).

> Where the target of the surveillance is a United States person, the FISA court may issue an order authorizing the surveillance only if the FISA judge concludes that there is probable cause to believe that the target of the surveillance is a foreign power or agent of a foreign power, that proposed minimization procedures are sufficient under the terms of the statute, that the certifications required by § 1804 have been made, and . . . that the certifications are not clearly erroneous.

Id. (citations omitted).

79. 50 U.S.C. § 1802.

80. *Id.* § 1802(a)(3).

81. *Squillacote*, 221 F.3d at 553.

> Each application to the FISA court must first be personally approved by the Attorney General. *See* 50 U.S.C.[] § 1804(a) [(2000)]. The application must contain, among other things, a statement of reasons to believe that the target of the surveillance is a foreign power or agent of a foreign power, specified information on the implementation of the surveillance, and a "certification" from a high-ranking executive branch official stating that the official "deems the information sought to be foreign intelligence information" and that the information sought cannot be obtained by other means.

Id.

82. Protect America Act of 2007, Pub. L. 110-55, 121 Stat. 552 (codified at 50 U.S.C. §§ 1805(a)–(c)).

83. *Id.*

communication is in electronic storage[84] for less than one hundred and eighty days, government entities must obtain a warrant[85] to compel the electronic communications service providers that own the data storage equipment to produce the records.[86] Where the content of the communication is in electronic storage for more than one hundred eighty days, government entities may obtain either a warrant, an administrative subpoena,[87] or a court order[88] to compel service providers to produce the electronic records.[89] Generally, notice to the subscriber or customer is not required.[90]

---

84. Generally, the ECPA distinguishes between an electronic communication in transit and one held in electronic storage. For a discussion of possible modifications to the ECPA that would clarify the difference between communications in transit and in electronic storage, see Steere, *supra* note 37.

85. Under the Federal Rules of Criminal Procedure, a warrant may be obtained for "evidence of a crime," "contraband, fruits of crime, or other items illegally possessed," "property designed for use, intended for use, or used in committing a crime," or "a person to be arrested or a person who is unlawfully restrained." FED. R. CRIM. P. 41(c). "After receiving an affidavit or other information, a magistrate judge or a judge of a state court of record must issue the warrant if there is probable cause to search for and seize a person or property under Rule 41(c)." FED. R. CRIM. P. 41(d).

86. 18 U.S.C. § 2703(a) (2006).

> 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.

Id.

87. To issue an administrative subpoena, the Assistant Director of the FBI may "request the name, address, length of service, and toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made" that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." *Id*. § 2709(b)(2).

88. To obtain a court order, the governmental entity must produce "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." *Id*. § 2703(d). The "specific and articulable facts" court order was introduced in the Communications Assistance for Law Enforcement Act of 1994, Pub. L. 103-414, § 207, 108 Stat. 4279, 4292.

89. 18 U.S.C. § 2703(b) (2006). "A governmental entity may require a provider of remote computing service to disclose . . . if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant," or if 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 "obtains a court order." *Id*.

90. *See Miller*, 425 U.S. 435 (holding that a bank customer has no standing to prevent disclosure of bank records). More generally,

> A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication, as specified by statute, 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, with prior

The ECPA also authorized the Director of the Federal Bureau of Investigation (FBI) to issue a national security letter (NSL) in the form of an administrative subpoena to requisition data regarding domestic terrorism.[91] That provision further prohibits certain disclosures of the receipt of, as well as compliance with, an NSL.[92]

Another provision[93] of the ECPA regulates the acquisition of routing information by the use of pen registers[94] and trap and trace devices.[95] To use such a device, investigators must obtain a court order pursuant to ECPA or FISA.[96] As with Title III, there are few exceptions.[97] Pursuant to ECPA, government attorneys and state law enforcement officers may apply to a court of competent jurisdiction[98] for an order authorizing the installation and use of a pen register or a trap and trace device provided that "the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[99]

> notice from the governmental entity to the subscriber or customer if 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 obtains a court order for such disclosure, as specified, except that delayed notice may be given pursuant to a specified provision. Furthermore, it is provided by statute that a governmental entity may require a provider of remote computing 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 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; obtains a court order for such disclosure as specified by statute; has the consent of the subscriber or customer to such disclosure; submits a formal written request relevant to a law-enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing; or seeks information under the specified provision.

AM. JUR. 2D *Computers and the Internet* § 9 (2004).

91. 18 U.S.C. § 2709(b) (2006).

92. *Id*. § 2709(c). However, see text Part II.B.2.b.

93. Pen Register Act, 18 U.S.C. §§ 3121–3127 (2006).

94. Under the statute, a pen register is defined broadly. It is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." *Id*. § 3127(3).

95. A trap and trace device is "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." *Id.* § 3127(4).

96. *Id.* § 3121(a).

97. *Id*. § 3122(b).

98. A court of competent jurisdiction is "any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated," or "a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device." 18 U.S.C. § 3127(2).

99. *Id.* § 3122(b)(2).

Recent case law suggests courts have begun to read the provisions of ECPA dealing with stored communications against a more rigorous application of the Fourth Amendment.[100] However, other courts have found it not unreasonable for the government to rely on ECPA provisions to seize data, and have upheld ECPA's refusal to extend an exclusionary rule to this arena.[101]

The ECPA established some procedural safeguards by requiring a warrant, an administrative subpoena, or a court order, which protects users' data in the possession of third parties.

b. USA PATRIOT Act

In the wake of the terrorist attacks of September 11, 2001, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT Act).[102] The PATRIOT Act expanded the Federal Rules of Criminal Procedure to allow warrants and administrative subpoenas to be issued for any "tangible things," "in an investigation of domestic terrorism or international terrorism."[103] The PATRIOT Act modified the ECPA such that a warrant for electronic information stored for less that one hundred eighty days had to be honored in other jurisdictions.[104] The PATRIOT Act expanded the ECPA to reach records of session times and durations, the types of services utilized, temporarily assigned network address, and the user's means and source of payment.[105] The PATRIOT Act expanded the voluntary disclosure provisions of the ECPA to include situations where "the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person."[106] The effect of these changes is not clear.[107]

---

100. *See Warshak*, 490 F.3d at 482.

101. *See* United States v. Ferguson, 508 F. Supp. 2d 7, 9–10 (D.D.C. 2007).

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

103. FED. R. CRIM. P. 41(b)(3).

104. USA PATRIOT Act § 220.

105. *Id.* § 210. For a more detailed analysis of the major modifications, see EFF Analysis of the Provisions of the USA PATRIOT Act (Oct. 31, 2001), http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php.

106. USA PATRIOT Act § 212.

107. It has been argued that

> The Patriot Act did not expand law enforcement powers dramatically, as its critics have alleged. In fact, the Patriot Act made mostly minor amendments to the electronic surveillance laws. Many of the amendments merely codified preexisting law. Some of the changes expanded law enforcement powers, but others protected privacy and civil liberties. Several of

The PATRIOT Act expanded the authority of the FBI to issue an NSL to include any situation "relevant to an authorized investigation."[108] In March 2007, the Department of Justice Office of the Inspector General declassified a report on FBI abuse of NSLs.[109] Also in March 2007, the PATRIOT Act amended the definition of "wire communication" in Title III by removing from its purview "any electronic storage of such communication."[110]

c. The USA PATRIOT Improvement and Reauthorization Act

A statute is only valid if it comports with the Constitution.[111] In *Doe v. Ashcroft*,[112] the U.S. District Court for the Southern District of New York held that the non-disclosure provisions of ECPA section 2709 contravened the Fourth Amendment; the provisions at issue effectively barred judicial review both of the non-disclosure provisions in NSLs that request the production of documents and of the merits of the request.[113] After

---

> the most controversial amendments may actually increase privacy protections, rather than decrease them. Most importantly, none of the changes altered the basic statutory structure of electronic surveillance law created by the Electronic Communications Privacy Act of 1986.

Orin S. Kerr, *Internet Surveillance Law After The USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 608 (2003). There could be a good argument for this position; however, it is beyond the scope of this Note.

108. 18 U.S.C. §§ 2709(b)(1)(A) and (2)(A) (2006).

109. U.S. DEP'T OF JUSTICE OFFICE OF THE INSPECTOR GENERAL, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS (Mar. 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf. At the time of this writing, the reaction to the abuse is not yet known.

110. PATRIOT ACT § 209, 115 Stat. 272, 283 (2001). "The USA PATRIOT Act deleted this phrase and amended § 2703 of ECPA to ensure that stored wire communications (e.g., voice mails) are covered not under Title III, but instead under the ECPA provisions that also apply to stored electronic communication, or e-mails." U.S. DEP'T OF JUSTICE OFFICE OF LEGAL EDUCATION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § IV.D.2 (2002).

111. "The general rule is that an unconstitutional statute, whether federal or state, though having the form and name of law, is in reality no law, but is wholly void, and ineffective for any purpose." Donald T. Kramer, *Total Unconstitutionality*, AM. JUR. 2D *Constitutional Law* § 203 (1998).

112. 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

113. In reaching its holding, the court looked to the development of the law surrounding administrative subpoenas, and concluded that

> because administrative subpoenas are 'at best, constructive searches,' there is no requirement that they be issued pursuant to a warrant or that they be supported by probable cause. Instead, an administrative subpoena needs only to be 'reasonable,' which the Supreme Court has interpreted to mean that (1) the administrative subpoena is 'within the authority of the agency;' (2) that the demand is 'not too indefinite;' and (3) that the information sought is 'reasonably relevant' to a proper inquiry.

Ashcroft, 334 F. Supp. 2d at 495, *vacated*, Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006) (citing United States v. Morton Salt Co., 338 U.S. 632, 652 (1950)). *See also* Oklahoma Press Pub. Co. v. Walling,

considering the text of various bills pending in Congress, the District Court recommended several provisions necessary to overcome the presumptive unconstitutionality of ECPA section 2709(c).[114]

In 2005, Congress considered these recommendations[115] when passing the USA PATRIOT Improvement and Reauthorization Act.[116] The Act enabled recipients of administrative subpoenas, among other things, to

---

327 U.S. 186, 208 (1946) (holding that "[t]he gist of the protection is . . . that the disclosure sought shall not be unreasonable"). Analyzing the court's opinion, one commentator has written:

> Where 18 U.S.C.[] § 2709 authorized the [FBI] to compel communications firms, such as internet service providers (ISP) or telephone companies, to produce, pursuant to the issuance of a [NSL], certain customer records whenever the FBI certified that those records were 'relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities,' in Doe v. Ashcroft, 334 F. Supp. 471 (S.D.N.Y. 2004), involving challenges to the statute by an internet access firm that had received a letter under the statute, the court held that 18 U.S.C.[] § 2709 might, in a given case, violate a subscriber's First Amendment rights of anonymous speech and association if judicial review was not readily available to an ISP that received an NSL. For example, the court observed, the FBI theoretically could issue to a political campaign's computer systems operator an NSL, under 18 U.S.C.[] § 2709, compelling production of the names of all persons who had email addresses through the campaign's computer systems, or it theoretically could issue an NSL under 18 U.S.C.[] § 2709 to discern the identity of someone whose anonymous online web log (blog) was critical of the government. The court said that such inquiries might be beyond the permissible scope of the FBI's power under 18 U.S.C.[] § 2709 because the targeted information might not be relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, or because the inquiry might be conducted solely on the basis of activities protected by the First Amendment.

Jay M. Zitter, Annotation, *Constitutionality of National Security Letters Issued Pursuant to 18 U.S.C.A. § 2709*, 2006 A.L.R. FED. 2d 3 § 3.

114. *Ashcroft*, 334 F. Supp. 493 ("Several bills pending in Congress, including H.R. 3179 [108th Cong. (1st Sess. 2003),] demonstrate Congress's and the Government's recognition that the NSL statutes could have been drafted with greater particularity and uniformity. H.R. 3179 would address two of the issues listed above by explicitly providing for judicial enforcement of NSLs and by imposing criminal penalties of up to five years' imprisonment for persons who unlawfully disclose that they have received an NSL.").

115. The House Judiciary Committee's Report spent many pages reviewing the court's holding and justifying the proposed amendments to the NSL procedures. H.R. REP. NO. 109-174(I) (2005). Specifically, the Judiciary Committee concluded that,

> [i]n the 108th Congress, Chairman Sensenbrenner introduced H.R. 3179, in part to address the fact that some NSL had explicit enforcement mechanisms and others did not. The Court in Doe v. Ashcroft concluded that there were three problems with NSLs: 1) the statute did not clarify whether consulting an attorney would violate the prohibition on disclosure under the law, 2) the statute contained no explicit provision for the Government to seek judicial enforcement, and 3) there was no provision imposing penalties against a person who fails to comply with an NSL. The Court found that 'H.R. 3179 would have addressed two of the issues listed above by explicitly providing for judicial enforcement of NSL's and by imposing penalties of up to five years' imprisonment for persons who unlawfully disclose that they have received an NSL.

Id. at 40–41 (citing *Ashcroft*, 334 F. Supp. 493).

116. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 115, 120 Stat. 192 (2006) (codified at 18 U.S.C. § 3511).

seek judicial review of those subpoenas.[117] Due to the legislation, in *Doe v. Gonzales*,[118] the Second Circuit Court of Appeals vacated and remanded *Ashcroft*, finding that the new judicial review provisions[119] rendered the constitutional violation moot.

On remand, the U.S. District Court for the Southern District of New York held revised sections 2709 and 3511(b) unconstitutional under the First Amendment as well as the doctrine of separation of powers.[120] The court found that section 2709(c) "functions as a licensing scheme that does not afford adequate procedural safeguards" and "cannot be severed from the remained of the statute."[121] The court, however, stayed enforcement of the judgment pending appeal.[122]

In sum, government entities must respect citizens' Fourth Amendment rights by obtaining a warrant, subpoena or court order for an electronic record. If a government entity believes the record relates to communication between foreign powers, a court order is still required if the target is a United States person. Presently, if a government entity believes the record relates to domestic or international terrorism, it may issue an administrative subpoena. But, the recipient of an NSL issued pursuant to an administrative subpoena may seek judicial review.

---

117. Specifically, the statute provides that

> The recipient of a request for records, a report, or other information under section 2709(b) . . . may, in the United States district court for the district in which that person or entity does business or resides, petition for an order modifying or setting aside the request. The court may modify or set aside the request if compliance would be unreasonable, oppressive, or otherwise unlawful.

18 U.S.C. § 3511(a) (2006).

118. 449 F.3d 415.

119. *See* 18 U.S.C. § 3511.

120. Doe v. Gonzales, 500 F. Supp. 2d 379, 425 (S.D.N.Y. 2007).

121. *Id.* The court found that "The revised provision incorporates case-by-case analysis in the determination as to whether nondisclosure of a particular NSL is necessary under the circumstances, but it continues to authorize nondisclosure orders that *permanently* restrict an NSL recipient from engaging in *any* discussion related to its receipt of the NSL." *Id.* at 420. On this point, the court concluded:

> The government's urging that an endless investigation leads logically to an endless ban on speech flies in the face of human knowledge and common sense: witnesses disappear, plans change or are completed, cases are closed, investigations terminate. Further, a ban on speech and a shroud of secrecy in perpetuity are antithetical to democratic concepts and do not fit comfortably with the fundamental rights guaranteed American citizens. Unending secrecy of actions taken by government officials may also serve as a cover for possible official misconduct and/or incompetence.

Id. at 421–22.

122. *Id.*

Interestingly, the Supreme Court has commented before on warrantless surveillance in the name of national security.[123]

C. Application of the Present Law

In our story, the husband of the woman in Kadiköy is an asylum-seeker and his wife requires secure communication, lest she be subjected to the persecution they fear. She might just have been a United States citizen ordering a birthday cake for her daughter, fearing the exposure of her credit card information and the coordinate damage of identity theft. She might also have been a member of a separatist group organizing a terrorist plot.

Each governmental actor has an articulable need to discover information respecting access to the Tor server in Portland. Which actors have the authority to gain access to the server is a function of a complex matrix of statutory capabilities and constitutional obligations. Access via that matrix depends on the purpose of the invasion, the identity of the subject and the nexus between the two. Further, there may or may not be any discoverable information transmitted or maintained by each server.

The local police officer, Detective Copal, is clearly conducting an ongoing investigation. As the content of the communication has been in electronic storage for less than one hundred and eighty days, there is, per se, a reasonable expectation of privacy pursuant to the ECPA. Detective Copal must obtain a search warrant from a magistrate judge or a judge of a state court of record by submitting an affidavit evidencing probable cause to search for and seize the property. To evidence probable cause, Detective Copal must show that searching the server logs and related service

123. In *Berger*, 388 U.S. at 114–15 (White, J., dissenting), Justice White opined:

> It is true that the Department of Justice has now disowned the relevant findings and recommendations of the Crime Commission, see Hearings on H.R. 5386 before Subcommittee No. 5 of the House Committee on the Judiciary, 90th Cong., 1st Sess., ser. 3, at 308 (1967) (hereafter cited as "House Hearings"), and that it has recommended to the Congress a bill which would impose broad prohibitions on wiretapping and eavesdropping. But although the Department's communication to the Congress speaks of "exercis(ing) the full reach of our constitutional powers to outlaw electronic eavesdropping on private conversations," the fact is, as I have already indicated, that the bill does nothing of the kind. Both H.R. 5386 and its counterpart in the Senate, S. 928, provide that the prohibitions in the bill shall not be deemed to apply to interceptions in national security cases. Apparently, under this legislation, the President without court order would be permitted to authorize wiretapping or eavesdropping "to protect the Nation against actual or potential attack or other hostile acts of a foreign power or any other serious threat to the security of the United States, or to protect national security information against foreign intelligence activities." H.R. 5386 and S. 928, § 3.

provider records will with some quanta of certainty lead to evidence of the crime. Such a showing should turn on the content of the suspicious e-mail message, evidence corroborating the authenticity of that message, the scope of the search and seizure request, and the government actors' familiarity with the technology. Though it is unlikely that the source of the message can, technologically, be determined with any certainty, a judge would likely authorize such a search or seizure. Pursuant to the USA PATRIOT Act, Detective Copal would be able to request from the Tor server owner's service provider records of session times and durations, the types of service utilized, the server's temporary or permanently assigned network address and the means and source of payment.

The FBI agent, Agent Fabian, is also conducting an ongoing investigation. Like Detective Copal, Agent Fabian may seek a warrant pursuant to the provisions of the ECPA. Of note, the USA PATRIOT Act expanded the jurisdiction of the issuing court by requiring other jurisdictions to honor a warrant issued pursuant to the ECPA.

In addition to the ECPA warrant inquiry, Agent Fabian has another tool available to her: administrative subpoena.[124] Pursuant to the ECPA, as modified by the USA PATRIOT Act, the requisitioning of information by an NSL is only authorized in the course of an investigation surrounding domestic terrorism. However, until the passage of the USA Patriot Improvement and Reauthorization Act, recipients of NSLs were not able to seek judicial review or even disclose receipt of an NSL, provided that the FBI simply avowed a terrorism related purpose. Although the FBI now has to justify such action, and although judicial review is now available, compliance with such discovery methods may continue *in terrorem*. The use of NSLs, triggering a system of administrative subpoenas with little judicial review, has aroused a great deal of controversy pitting arguments for privacy rights against arguments for security. In fact, in March 2007, the Department of Justice Office of the Inspector General released a report scrutinizing the FBI's misuse of NSLs to this end.[125] In September 2007,

124. Laws specific to child pornography investigations exist, authorizing the search and seizure of sites providing such content, but they do not extend to the third parties involved here: the provider of the public message board and the owner of the Tor server. *See, e.g.*, Child Pornography Prevention Act of 1996, 18 U.S.C. § 2256 (2006).

It is interesting to compare the recent seizure of Tor servers by German authorities in connection with a child pornography investigation. *See TOR Anonymizing Proxy Servers Seized in Germany on Child Porn Charges*, http://arstechnica.com/news.ars/post/20060911-7709.html (last visited Sept. 11, 2007). For a community of Tor users' perspectives, see *Germany: Crackdown on TOR-node Operators*, Sept. 10, 2006, http://itnomad.wordpress.com/2006/09/10/germany-crackdown-on-tor-node-operators/.

125. *See supra* note 99.

the U.S. District Court for the Southern District of New York held such NSLs to be unconstitutional, although that judgment has been stayed pending appeal.[126]

To install a pen register or trap and trace device, pursuant to the ECPA, or to intercept future communications related to the child pornography ring, pursuant to Title III, Agent Fabian would need an Assistant U.S. Attorney in the District of Colorado to obtain a court order from the District Court of Colorado or the Tenth Circuit Court of Appeals. Even if Agent Fabian can demonstrate a nexus between the Tor exit point and a crime, she would have a hard time obtaining such a court order. In particular, as Agent Fabian does not know the identity of the individual initiating communications, she would have a hard time meeting the intercept order's particularity requirement. Given the nature of communications on the Tor network, Agent Fabian would also struggle to comply with the pen/trap order's prohibition on content interception. In this context, the statutes at issue require a retroactive and not proactive investigative tact.

Finally, the NSA agent, Agent Nasal, is also conducting an ongoing investigation. Both the ECPA and FISA, as modified by the USA PATRIOT Act, allow certain modes of discovery where the governmental entity is engaged in an investigation of domestic or international terrorism.

The ECPA would likely permit Agent Nasal to obtain a warrant for the search and seizure of the server in Portland provided she can show probable cause, not with respect to evidence of a crime but, rather, of a nexus between the tangible things and a terrorist plot. Further, with respect to terrorism, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person is imminent, the ECPA permits the service provider, as well as the owner of the server, to voluntarily disclose the records.

Agent Nasal has powers respecting interception, pen registers, and trap and trace devices, unavailable to Agent Fabian because Agent Nasal is engaged in an investigation into terrorism. It is unlikely, however, that this investigation warrants the use of those powers. FISA requires that Agent Nasal know the communication is between or among foreign powers with some level of certainty. Though Agent Nasal is able to act without the prior approval of the FISA Court, it is unlikely that Agent Nasal could show sufficient evidence of governmental action. Agent Nasal knows only

126. *See* text accompanying notes 120–22.

that packets were transferred between a server in Japan and one in the United States.

Since it is unknown whether the surveilled party is a United States person, a court order is required. Here, Agent Nasal faces issues similar to those faced by Agent Fabian. Agent Nasal would have to show the target is a foreign power or that the more standard probable cause requirement is met.

It is unclear how the Protect America Act, respecting domestic surveillance pursuant to FISA, will affect Agent Nasal's terrorism investigation. Additionally, at the time of this writing, the extrajudicial surveillance techniques employed by the NSA are unknown.

Although the statutes may permit the governmental actor to search and seize information in certain cases, those statutes may be challenged as violative of constitutional rights. For example, if the woman in Kadiköy is a United States citizen simply purchasing a birthday cake for her daughter in Missouri, a strong argument exists that she has a reasonable expectation of privacy in her communication, especially as evidenced by her use of the Tor network. Such a reasonable expectation of privacy implicates due process rights, which entitle her to notice and an opportunity to be heard before existent records of her activity are disclosed.

Further, as should be clear through the examples, the technology itself is capable of ensuring privacy, even where the Constitution fails.[127] Tor servers do not, by default, maintain any logs of transmitted packets.[128] Having captured packets in the Tor network, a governmental actor will be unable to discern the content and routing of those packets. Even if Agent Nasal operates her own Tor server, she would be unable to peel back the layers of the onion.

III. A SCHRÖDINGER'S ONION APPROACH TO SECURE INTERNET COMMUNICATIONS

As the previous section should have made clear, a baseline shift is required. Our constitutional analysis, informed by analogies drawn from the law of real property, breaks down where packets' owners are

127. It is important to note that this is a different argument than Professor Reidenberg advanced in his influential article, *Lex Informatica*. *See infra* note 132.

128. The Tor server does not keep activity logs. Of note, while there is currently no statute requiring the maintenance of logs by service providers, "[t]he Justice Department is asking Internet companies to keep records on the Web-surfing activities of their customers to aid law enforcement, and may propose legislation to force them to do so." Saul Hansell & Eric Lichtblau, *U.S. Wants Companies to Keep Web Usage Records*, N.Y. TIMES, June 2, 2006, at A15.

unidentifiable and no coordinate right to exclude is cognizable. Similarly, our statutory framework, operating to animate these unassignable principles, serves to authorize and prohibit governmental entities' access in counterintuitive ways, especially where the parties involved, the content and the nature of the communication are unknown. In the above examples respecting the asylum-seeker's use of the Tor network, although it is likely that each governmental actor would be authorized to access stored records, it is unlikely that any would be authorized to intercept potentially crucial information. (The NSA agent might nonetheless, depending on exigency, have resort to extrajudicial capabilities.) And none of the governmental actors would likely be able to overcome the bar to access created by the technology itself.

Faced with a need to adapt our privacy laws to the age of the Internet, which institution is best able to do so? In 2004 and 2005, Professors Kerr and Solove argued this point. Professor Kerr argued that legislatures do and should dictate privacy law for reasons of institutional competence.[129] In reply, Professor Solove argued "that [Professor] Kerr is too quick to extol the virtues of Congress and that he is especially misguided in suggesting that courts take a back seat to legislatures in creating criminal procedure rules for new technologies"; rather, Professor Solove would have the courts "hold that the Fourth Amendment applies, and then determine whether Congress's legislation is adequate to satisfy the Fourth Amendment."[130] Professor Kerr responded to the critique by asserting that Professor Solove's "institutional comparison contrasts statutory rules as they are with constitutional rules as he wishes them to be," and that his "legal framework matches his normative policy preferences."[131] In 1998, Professor Reidenberg introduced a third point: "Lex Informatica may also

129. Professor Kerr argued that statutory rather than constitutional rules control and this is preferable because, in the criminal context, restrictions created by legislatures provide more certainty and reflect more majority preferences than those created by courts, and statutory rules "will tend to be more sophisticated, comprehensive, forward-thinking, and flexible than rules created by the judicial branch." Kerr, *supra* note 17, at 859–60.

130. Solove, *supra* note 62, at 761, 774. Specifically, Professor Solove argued that court-made rules are flexible, accounting for a balancing of interests, whereas statutes lack effective remedies, are often unclear, not self-executing, underprotective of Fourth Amendment rights, and fail to predict, ex ante, technological innovations. *Id.* at 762–71.

131. Orin S. Kerr, *Congress, the Courts, and New Technologies: A Response to Professor Solove*, 74 FORDHAM L. REV. 779, 781 (2005). Comparing the institutional competency of the courts with that of Congress, Professor Kerr drew an analogy: "Judges follow a closed-source model, in which they ask for briefs, hold a short oral argument, and then work in secrecy to produce the outcome. Legislatures follow an open-source model, in which the language and procedure is open to the public." *Id.* at 783. Concluding, Professor Kerr expressed doubts that "courts have the capacity to review such statutes in a coherent and principled way." *Id.* at 790.

substitute for law when technological rules are better able to resolve policy issues."[132]

And what should that institution assume? The widespread use of Voice-Over-IP technology, Internet telephony, further illustrates why an a priori assumption is necessary. Voice-Over-IP telephony packets are transferred over the public Internet. In the context of Title III, it is unclear whether such technologies would need to be intercepted as "oral" or as "electronic" communications. Even if this were an easy question for the courts to decide where the parties involved, the content and the nature of the communication are known, it is less clear where Internet telephony occurs across an encrypted tunnel, and even less clear when these packets are transferred through the Tor network. Given the lack of knowledge, the preliminary assumption warranted by the Fourth Amendment, or the choice of statute relied on by the governmental actor, would likely control the court or administrator's decision. The preliminary decision is crucial given the absence of an exclusionary rule respecting the interception of electronic communications.

I propose we begin our thinking about how to animate the constitutional principles at issue by considering a Schrödinger's Onion approach. Despite their disagreement about which institution is best suited to serve as primary locutor, Professors Kerr and Solove agree, as do I, that one of the institutions must establish, before it is too late, sufficiently protective rules.[133] I contend that it does not matter which institution does so, be it Congress, the courts, or the information industry itself. What is crucial, however, is that each institution internalizes a new presumption-one that bears on our preliminary definitions. Without evidence to the

---

132. Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 583 (1998). Specifically, Professor Reidenberg argued that technology marginalizes the effectiveness of legal regulation:

> First, technological developments outpace the rate of legal evolution. Consequently, today's regulations may easily pertain to yesterday's technologies. Second, today's technology may limit the ability of government to regulate. For example, digital networks can no longer be wiretapped like analog phone systems. And finally, information flows may be impervious to the actions of a single government. As pundits have observed, the United States Constitution may just be a speed bump on the Information Superhighway.

Id. at 586 (citation omitted).

133. Professor Solove noted: "To the extent that [Professor] Kerr is urging courts to apply basic Fourth Amendment principles and be open to allowing legislatures to fill in the details, his advice is sound." Solove, *supra* note 62, at 776. Professor Kerr agreed: "Existing law contains a number of gaps, Solove explains; it does not offer enough protection and its remedial schemes are inadequate to protect privacy. . . . I agree with a number of these criticisms, and, as Solove notes, have written articles making similar points." Kerr, *supra* note 131, at 782.

contrary, we must presume all Internet packets relate to U.S. citizens and are entitled to the highest protection.

CONCLUSION

The competition of citizens' interests in safeguarding constitutional rights as well as in ensuring security, of foreign nationals' interest in having basic liberties respected, and of governmental entities' needs to wage effective wars on crime and terrorism creates a storm-laden atmosphere. The debate is brought into greater contrast where growing use of encryption introduces information problems by technology rather than law.

To protect citizens' First, Fourth, Fifth and Fourteenth Amendment rights, all electronic communications and records subject to Title III, the ECPA, and FISA must be presumed to belong to United States citizens. However, even where it is unclear whether the law will always protect these privacy interests, it is clearer that technology will not always permit publicity. We must navigate where the air is thinnest. The Internet was developed with an eye to nuclear survivability and has greatly exceeded expectations. What is more, though we can have great confidence in our technology's capacity to outlast catastrophe, we must affirmatively ensure our Constitution can do the same.

Joshua A. Altman[*]

---

* A.B. (2002), Duke University; J.D. Candidate (2008), Washington University School of Law. In particular, I would like to thank Professor Neil Richards. There are too many other wonderful people to thank at Washington University Law for me to list them all by name. Thank you for being mentors, friends, and readers, for providing encouragement, and sound advice, and for caring.