# WARRANTLESS SEARCH AND SEIZURE OF E-MAIL AND METHODS OF PANOPTICAL PROPHYLAXIS

Paul Ham [1]

## I. INTRODUCTION

### A. *The Fourth Amendment and the Protection of Privacy in Electronic Communications*

U.S. citizens are in a constant battle for their rights to privacy, fighting the government's increasingly pervasive surveillance and justicial needs. One area where court opinions conflict with the public's expectation of privacy is over the realm of personal electronic communications. The general public believes electronic communications must be afforded a certain level of privacy that is not currently recognized by case law or statutes. [2] Under current case law, warrantless searches and seizures of your personal e-mail are not prohibited by the Fourth Amendment. [3]

Fueling the public's disconnect is the fact that technology progresses faster than the law. [4] The Constitutional Framers did not consider the depth and variety of technology used daily by every individual, nor did they predict the repercussions their words would have upon new technological uses. [5] Congress did not anticipate the widespread, various uses of electronic communications when they drafted much of the applicable legislation. [6] Furthermore, most courts rely upon legal reasoning that only tenuously analogizes between traditional methods of communication or privacy protections in light modern electronic communications. [7]

Based upon this legal backdrop, courts generally refuse to recognize society's expectation of privacy over electronic communications. [8] Courts still hold onto outdated legal analyses for outdated technologies--and apply them as best they can to the burgeoning world of new technologies. [9] As a result citizens must turn to extralegal protections, such as implementing various technologies to circumvent legal prescriptions. Individuals must work with these new technologies to protect their Fourth Amendment rights.

The classic two-prong test in judging whether the Fourth Amendment protects an individual's right to privacy asks: (1) whether the individual expects privacy, and then (2) whether society finds this expectation reasonable. [10] The first prong, the subjective expectation of privacy, is difficult to contest because a defendant will almost invariably affirm that expectation. [11] Therefore, the second prong is what courts generally focus upon. [12] Yet it is this second prong that most often flies in the face of what the general public accepts--that courts' interpretations of the Constitution do not reflect the subjective expectations of society.

Thus, where case law and statutory reforms have continually narrowed privacy protections over electronic communications, the citizenry's only option is to demonstrate to the courts and the legislature how they wish their rights to be preserved. [13] Until then, this paradox of perceived privacy rights drives individuals to implement extralegal technical methods such as encryption and anonymization to protect what they perceive to be theirs by right. Whether the courts and legislature follow these trends is an issue that needs to be decided sooner rather than later. [14]

For the purposes of this article, electronic communications will be narrowly limited to electronic mail (“e-mail”) and in some cases also instant messaging communications (“IM”) or similar “one to few” messaging systems. American Jurisprudence defines electronic communications as “the exchange of ideas, messages, or information, by written word, and includes information communicated to or received by an individual and information communicated concerning an individual's Internet usage.” [15] Practically speaking, this includes, at the least, e-mail, web-browsing histories, instant messenger communications, participation in synchronous “chat rooms” or asynchronous “bulletin board” messaging systems (“bulletin boards”), “buddy lists,” and address books. The scope of this accepted definition is too broad for the purposes of this article. In many cases, the technology and implementation may be sufficiently similar to merely extend the legal reasoning here to understand the protections afforded them.

### B. *Framing Hypothetical: You and Your Eco-Terrorist Friend*

Consider a hypothetical: You are an environmental rights activist. One of your colleagues is a suspected eco-terrorist. Now your electronic communications are under investigation in connection with local eco-terrorist activities. Whether or not you are in communication with this suspected eco-terrorist, are your e-mails protected from warrantless search and seizure? If not, then what can you do to protect your own expected right to privacy over your e-mail?

The Fourth Amendment should be your source for protecting your e-mails when you are under scrutiny as a private citizen in a public cyberspace. Regardless of whether you have anything potentially illegal in your e-mail, you suspect that you have the right to be notified by a warrant of any search of your e-mail. A warrantless search of your e-mail, revealing private thoughts and details to strangers, may open you up to the type of indignity similar to that prohibited in *Terry v. Ohio*. [16] Yet, courts have refused to grant the contents of e-mail this Constitutional protection.

The remainder of this article will examine the case law and statutes controlling this situation and examine technological implementations that may protect your expectation of privacy in light of your exposure to the eyes of the government. It will then explore this lack of privacy as the type of panoptical society described by the philosophers Jeremy Bentham and Michel Foucault. Finally, it will close with a discussion of methods of "panoptical prophylaxis"--what extralegal technologies are available to individuals interested in protecting their privacy? Also, this article will discuss the issues of privacy and communications in virtual world environments and their effects on "real world" privacy expectations and protections.

## II. DISCUSSION

### A. *The Supreme Court on Privacy*

The Supreme Court has yet to make a definitive ruling regarding the Fourth Amendment protection of electronic communications. Until then, lower courts have relied upon a number of other decisions related to privacy, applying those cases in the context of the Internet. In *Katz v. United States*, the Court created the foundational two-prong test for determining an individual's right to a reasonable expectation of privacy. [17] In *United States v. Jacobsen*, the Court conceded that the warrantless search and seizure of a letter or package by law enforcement is unconstitutional. [18] Lastly, the Court in *Kyllo v. United States* tackled the issue of technology impinging upon privacy rights in a novel way, deciding in that case that the specific use of technology violated the Fourth Amendment. [19]

### B. *Katz v. U.S. -- Not the Intruding Eye, but the Uninvited Ear*

#### 1. The Case

In *Katz*, the Supreme Court determined that the warrantless attachment of an electronic eavesdropping device to a public phone booth violated the phone user's Fourth Amendment right of a reasonable expectation of privacy. [20] Overturning the Court's famous decision in *Olmstead v. United States*, [21] the Supreme Court decided that the person--and not merely the space--is the object protected by the Fourth Amendment. [22] The Court deemed the petitioner's conversation private, and, after it was intercepted and recorded by the government, the evidence collected was disallowed as an illegal search and seizure. [23]

In concurrence with the decision, Justice Harlan articulated a two-part test to determine whether a reasonable expectation of privacy exists: (1) Does the individual have an actual expectation of privacy over his or her communication, and, most importantly, (2) is this expectation one that society is prepared to recognize as reasonable? [24] These key phrasings in *Katz* protect the right of privacy in the individual, and not of the space or the penetrability of that space. [25] "[What the individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." [26] What the individual sought to exclude was "not the intruding eye--it was the uninvited ear." [27]

 

The Court in *Katz* cautions that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." [28] In e-mail, the "eye" is the interception of the e-mail text through technologically necessary "middle-men," and the "ear" is the access and reading of that text. [29] Updating this statement through analogy, one might say that a narrow reading of the Constitution might ignore the vital role that the public *Internet* has come to play in private communication. Though the Internet at large may be considered a "public" social space, it is the content within the Internet that an individual seeks to preserve as private and that should be protected.

In essence, the exception that courts have made by distinguishing e-mail communications over a "public" Internet from private conversations within a "public" phone booth is the same exception the government unsuccessfully petitioned for in *Katz*. [30] The Supreme Court refused to allow the exception for a technological advancement in electronic wire-tapping. [31] Personal communications, wrapped in an e-mail and sent over the Internet should be no different than the private conversations in a public space protected in *Katz*. Yet, as explained below, courts contend that once a private e-mail is exposed to the public Internet--with its network of anonymous routers and other networked nodes--the sender knowingly gives up her privacy, thus avoiding the protections carved out in *Katz*.

2. *Commonwealth v. Proetto* -- The *Katz* One-Prong Test for a Right to Privacy

Various court decisions have modified the Katz two-prong test, rendering the first prong as practically moot, and relying wholly upon the second prong to test the constitutional scope of Fourth Amendment protections. [32] The Superior Court of Pennsylvania summarized the legal reasoning on the expectation of privacy of electronic communications in *Commonwealth v. Proetto*. [33] The *Proetto* court reduced the two-prong Katz test to the second prong, testing whether an individual's expectation of privacy is reasonable in light of all the surrounding circumstances. [34] Based upon this reasoning, the court held that e-mail, upon receipt, is no longer private since, like a paper-based letter, upon "opening" the contents are outside of the control of the sender. [35]

In *Proetto*, police officers arrested a fellow officer for criminal solicitation, possession of obscene and other sexual materials and performances, and corruption of minors for his electronic communications with a 15-year-old girl. [36] The electronic communications consisted of e-mails and chat room conversations. [37] The appellant moved to suppress the electronic evidence under a violation of his Fourth Amendment rights to privacy. [38] The court found no violation of the Fourth Amendment and denied the motion to suppress. [39]

Other courts similarly have held that no constitutionally reasonable expectation of privacy exists in e-mail. Their reasoning is largely based upon the fact that once a user sends an e-mail from his or her computer that e-mail is delivered immediately to a public Internet where Internet service providers ("ISPs"), other users, and potentially "hackers" or the government may access the text in transit. [40] The e-mail, since it is delivered over the Internet in plain text, [41] is more like a postcard than a letter in an envelope. [42] Next, for the e-mail to be delivered to a recipient, the e-mail provider records that e-mail, and, as a business record, that e-mail is open to governmental scrutiny. [43] Finally, the e-mail is sent to a private recipient who may easily forward that e-mail to the general public, a technological and social fact that is recognized by all e-mail users. [44] Courts assume that users sending e-mail are aware that their privacy begins to disintegrate at the moment it is sent out of their personal computers, through a public Internet, and completely evaporates the moment that e-mail is received. [45]

Yet, courts have held that a reasonable expectation of privacy exists for e-mails sent and received within an Internet service provider's services, such as America On-Line ("AOL"). [46] Since those cases were decided, however, e-mail has largely moved out of the limited realm of single ISPs like AOL, onto a public Internet with web-based mail and online accounts for technological reasons and popular demand. Courts have not found a reasonable expectation of privacy for such e-mails. [47] If an individual uses an alias in sending or receiving traditional mail, however, the expectation of privacy may be preserved. [48] Furthermore, courts in their legal reasoning have been inconsistent in ruling whether e-mails are private in transmission, between Internet servers, from the sender to the receiver.

Similarly, courts have determined that no reasonable expectation of privacy exists for communications over

 

bulletin boards or chat rooms. [49] It is arguable that communications via instant messenger may be more like private e-mails than postings on bulletin boards or chat rooms, therefore, a reasonable expectation of privacy may exist. On the other hand, the fact that many "chat" sessions are by default logged belies this expectation of privacy. [50]

From these cases, it is clear that there is no Fourth Amendment protection of privacy over e-mail, even though most lay people would expect otherwise. From the cases following *Katz*, the public expectation of privacy does not justify the actual recognition of that expectation. Again, the courts rely upon technical reasons and analogies from first-class mail to justify government intrusion into seemingly private communications.

3. The Eco-Terrorism Hypothetical -- No Privacy in E-mail

The case law is clear that once an e-mail is sent, the sender loses all Fourth Amendment protection of the contents. Therefore, the government generally need not obtain a warrant to peruse a private citizen's e-mail once that e-mail enters cyberspace. But are there other methods of obtaining legal protection for one's e-mail?

### C. *Kyllo v. U.S.* -- *Technological Changes and Their Effect on Privacy*

1. The Case

In *Kyllo v. United States*, the Supreme Court held that the use of thermal imaging devices to "search" a private residence is within the scope of Fourth Amendment protections, thus, requiring a warrant. [51] The use of the thermal imaging device constituted a search because it involved a sense-enhancing technology not in general public use and collected information that would otherwise require physical intrusion into the residence. [52] The evidence collected in this warrantless search was therefore excluded from trial.

The legal reasoning directly addressed the application of the Fourth Amendment with the progress of surveillance technology in search and seizure cases. [53] The Supreme Court held that technology should not "shrink the privacy the Fourth Amendment was originally designed to protect." [54] Furthermore, because the technology was not in general public use, "[t]o withdraw protection of this minimum expectation [of privacy] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." [55]

From this decision, one may excise the general understanding that new surveillance technologies must at least undergo higher scrutiny when applied to issues with privacy implications. Considering this, one might think that since the search and seize of private e-mails requires technology and techniques that may be outside of general public use, e-mail should be protected from warrantless search and seizure. Yet, cases such as *Proetto* conclude that this expectation is not one the courts will fulfill. Furthermore, since the technology does not collect information otherwise requiring physical intrusion to obtain, *Kyllo* offers no clear guidance to interception e-mail communications.

The *Kyllo* decision further raises the question as to whether e-mail in transit is within the auspices of the "plain view" doctrine--"[i]n the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes" [56]--later courts have not relied upon this reasoning to justify Fourth Amendment protection.

2. The Eco-Terrorism Hypothetical -- No Privacy in E-mail, Again

*Kyllo* may continue to offer some hope in higher scrutiny of new technologies and their power in monitoring private communications, but not yet. The general standards and guidelines for privacy have also not been upheld in later courts. Thus continues the search for other legal protections for one's e-mails in light of the hypothetical introduced at the start.

 

### D. *United States v. Jacobsen* -- *Truth in Packaging*

#### 1. The Case

In *United States v. Jacobsen*, the Supreme Court decided that the search and seizure of letters and closed packages, by law enforcement officers, requires a warrant under the Fourth Amendment. [57] In the case, Federal Express employees opened and examined the contents of a damaged package in their care. [58] Inside, they found a "white powder." [59] They subsequently notified the Drug Enforcement Administration. [60] A federal agent then tested the powder, determining it to be cocaine. [61]

The Supreme Court found the Federal Express search legal because a private actor instituted it. [62] On the other hand, if the search were performed by a law enforcement officer, a warrantless search would be "presumptively unreasonable." [63] The officer, under the Fourth Amendment, would require a warrant. [64] In *Jacobsen*, the drug enforcement officer's search was legal because it was subsequent to a private search by the Federal Express employees. [65] "The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." In *Jacobsen*, the Federal Express employees "frustrated" the expectation of privacy, and the law enforcement officer was thus legally able to commence his search. [66]

#### 2. The Eco-Terrorism Hypothetical -- A Glimmer of Hope, But a Tear in the Packaging

*Jacobsen* is relevant to the case at hand because, by analogy, e-mail is similar to a letter or a closed package in function, if not exact in form. If a package may be protected, how about an e-mail that has yet been "unopened" by the recipient? Would one's e-mails be protected at least up to the point where the recipient reads its contents? Unfortunately, courts have held that since the e-mail is not concealed--in fact, technically, it is delivered in "plain text" over the Internet--no analogy with packaging may be made.

### E. *The Wireless Cases* -- *Decisions in the Ether*

One defense that arises from time to time is the "wireless defense." In this defense, a party argues that because they access the Internet via an unsecured wireless router, any Internet traffic cannot be directly attributed to their personal use, but could with fair probability be attributed to other users. [67] An ISP assigns a unique IP, an Internet protocol address comprised of up to twelve numbers, to the router. Any computer that accesses the Internet through that router then assumes the single IP address of the router. Through this IP, someone can request from an ISP the identity of the subscriber who owns the router--but potentially not the identity of all the users who access the Internet through the router. Thus, Internet subscriber A may falsely be attributed with the Internet traffic of user B who happens to be in broadcast range of A's wireless router.

#### 1. *Bartnicki v. Vopper* -- The First Amendment Comes First

In *Bartnicki v. Vopper*, an unidentified individual intentionally intercepted and recorded a cellular phone conversation during a contentious teacher's union dispute. [68] Respondent Vopper, a radio commentator, then played the tape on the radio during his talk show. [69] The Supreme Court decided that the interception was unlawful under statute, yet the application of the statute in the present case violated the First Amendment, and the intercepted communication was deemed lawful. [70]

The decision in *Bartnicki* subordinates Fourth Amendment privacy concerns under First Amendment freedom of speech rights regarding intercepted cellular or cordless telephone conversations. [71] Furthermore, it shows that statutes may control the protection of communications intercepted over the wireless medium.

#### 2. *People v. Stone*

In *People v. Stone*, the Supreme Court of Michigan held that eavesdropping upon a cordless telephone

 

conversation betrayed the meaning of a "private conversation" under Michigan's eavesdropping statutes. [72] This decision goes against the grain of a U.S. Court of Appeals, Sixth Circuit, ruling in *McKamey v. Roach* that cordless telephone conversations afford no reasonable expectation of privacy for the users. [73] The *Stone* Court did not rely upon Fourth Amendment jurisprudence, but only sought to define "private conversation" in light of the state's eavesdropping statute. [74]

3. The Nevada Gamble

Two unpublished opinions from the U.S. District Court in Nevada, however, work to evaporate the wireless defense. In *U.S. v. Latham*, the court rejected a defendant's challenge to an affidavit supporting the government's search warrant of his premises, arguing, among other things, that the affidavit failed to address the chance that the defendant's wireless Internet connection could be intercepted. [75] In *U.S. v. Carter*, the court took up a substantially similar issue, but on this second take on the wireless defense, the same expert witness in *Latham* testified in *Carter*, adding the facts that occasionally communities and neighborhoods share wireless connections and thus the same IP addresses. [76] In *Carter*, the expert also added that sometimes people "drive around neighborhoods and office parks with laptop computers looking for open or unprotected wireless access points to the Internet." [77]

In both cases, the courts rejected the defendants' arguments, challenging the probability that the Internet traffic responsible for the charges were not fairly attributable to the ISP subscriber. "[E]ven if the information set forth in [the experts'] affidavits had been included ... there would still have remained a likelihood or *fair probability* that the transmission emanated from the subscriber's place of residence" and thus the search warrants would be justified. [78]

4. The Eco-Terrorism Hypothetical -- E-mails are Protected In-Transit from Wireless Interception

From *Bartnicki* and *Stone*, some additional protection from warrantless searches and seizures may be afforded to e-mail communications. An e-mail is protected while it is being composed, and while on a wireless network it is protected until it reaches a point that is "public." This point may be the wireless access point through which a sender's computer connects to an ISP. From that point on, however, the content of that e-mail message may be accessible. At the least, an e-mail is protected from nearby wireless eavesdropping, by statute, upheld by case law.

However, the wireless defense may not be available to persons suspected of prosecutable Internet transmissions. If an e-mail was intercepted in any situation, the IP address associated with that e-mail may be traced back to the subscriber of the Internet connection and then the content would be attributable to that subscriber. [79]

F. *Read the Fine Print, It Might Protect You*

1. *United States v. Long*

The strongest statement for Fourth Amendment protection of the public's perceived expectation of privacy over e-mail comes from *United States v. Long*. [80] In this case, the military searched and seized e-mails from the appellee, Long, containing evidence of drug use in violation of the Uniform Code of Military Justice. [81] These e-mails were sent and received on a government computer. [82] The court, reversing the lower court decision, determined that by its terms a log-on banner specifying the terms of use for the e-mail system [83] granted a reasonable expectation of privacy in e-mails sent and received on the system. [84]

In its decision, the *Long* Court relied upon appellee's use of a password, known only to her, and the language of the log-on banner. [85] The log-on banner described access to "monitor" the system, but "not to engage in law enforcement intrusions by examining the contents of particular e-mails in a manner unrelated to maintenance of the e-mail system." [86] Furthermore, the testimony of the network administrator of the system supported the agency practice of customarily recognizing the privacy of its e-mail users. [87] The search conducted by law enforcement officers for law enforcement purposes went beyond work-related monitoring or search for work-related misconduct, and thus required a probable cause. [88] The court ruled that the e-mail evidence against Long should have been suppressed. [89]

 

This case is limited by the scope of an employment situation. It does not venture into the technical intricacies of e-mail communications to the extent of *Proetto*. Instead, it stops short, declaring only that within a limited context, similar to e-mail sent within an ISP as in *Maxwell*, expectations of privacy may be reasonably recognized. [90] In fact, it is only in the dissent where constitutional Fourth Amendment jurisprudence is brought up to contest the majority decision. [91]

2. *NERA v. Evans*

In *National Economic Research Associates, Inc. v. Evans*, the Massachusetts Superior Court held that an expectation of privacy existed over e-mails on a work computer where the company's policies declared that visited web sites would be monitored, but not the content of Internet communications. [92] The court examined the privacy issues implicated in a motion to compel the production of attorney-client communications. NERA, the employer, argued that employees should know that NERA took "screen shots" of all web pages viewed, including password-protected web pages from a Yahoo! e-mail account. [93]

In the decision, the court took guidance from the American Bar Association, which concluded that "lawyers have a reasonable expectation of privacy when communicating by e-mail maintained by an [on-line service provider]." [94] The court recommended that if employers wished to destroy the attorney-client privilege then they must "plainly communicate to the employee that 1. All such e-mails are stored on the hard disk of the company's computer in a "screen shot" temporary file; and 2. The company expressly reserves the right to retrieve those temporary files and read them." [95]

This, along with *Long*, skirt a narrow line where employees seeking privacy protection of their e-mails must understand clearly the terms of use of their employers' Internet connections and employee manuals. The affordance of privacy is not explicit, but only thinly protected by the fine print.

3. The Eco-Terrorism Hypothetical -- Protection of Privacy in National Defense

Finally, the *Long* and *NERA* decisions offer distinct hope for courts recognizing a generalized, reasonable expectation of privacy in e-mail. These rulings, however, are very fact-specific. For example, with *Long*, privacy stands only in a certain employment context, with a log-on disclaimer on an internal e-mail system, with an administrative practice of respecting rights to privacy, and in a military court. The *NERA* decision focuses on the expectation of privacy, but specifically to protect the attorney-client relationship in e-mail communications.

Prospectively, these decisions show a shift in the nearly *carte blanche* denial of any reasonable expectation of privacy over e-mail. Furthermore, in *Long*, the majority exhibits a practical and realistic skepticism towards the actions of law enforcement. Where many Supreme Court decisions in the realm of criminal procedure tend to trust law enforcement officers as operating purely in the "peace," the *Long* Court questions the credibility of the government's witnesses. [96] Perhaps with cases such as *Long*[KAM1], courts will continue to pursue methods of protecting the realm of electronic communications from what the public perceives to be unreasonable searches and seizures.

### G. *Congressional Reforms*

Congress enacted a number of legislative reforms, attempting to clarify the extents and bounds of individual privacy over electronic communications. The Electronic Communications Privacy Act of 1986 ("ECPA") [97] attempted to codify privacy protections for law enforcement access in electronic communication, transmission, and storage. [98] Also, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "PATRIOT Act") [99] broadens the ability of the government to tap, search, and seize the communications of non-citizens suspected of terrorist activity--a scope that may also reach into the communications of citizens themselves.

The ECPA limits the scope of the Federal Wiretap Act, [100] making "unauthorized access, interception, or

 

disclosure of private communications of any kind illegal." [101] The ECPA requires probable cause and a warrant for accessing e-mail at the sender's terminal and the recipient's mailbox. [102] Yet, the ECPA created a new loophole for the government to access the contents of those e-mails. [103] Using a "business records" exception, supported by subsequent case law, a government official may access e-mail that has not been read by the recipient since it is allowed access to these e-mails as business records held by the ISP. [104]

The ECPA, combined with the Stored Communications Act, [105] government officials may only require a warrant, with no notice, prior or delayed, for e-mails held by an e-mail provider for more than 180 days. [106] A subpoena may be all that is necessary. Practically speaking, subpoenas are often issued with little judicial oversight. [107] This simply circumvents any protection under the Fourth Amendment for e-mail communications, since as a business record, the content of any e-mail sent through an e-mail provider no longer becomes the property of the sender. Furthermore, recent changes to the Federal Rules of Civil Procedure may require more stringent retention policies for businesses and their electronic documents. [108]

Currently, the PATRIOT Act allows the government to conduct warrantless searches and seizures of electronic communications of non-citizens. Yet the PATRIOT Act may also extend FISA to allow the warrantless search and seizure of communications of non-terrorist citizens if involved in a criminal investigation. [109] While this theory has not yet been tested, there are many indicators that the government may apply it in the near future in its efforts to combat terrorism through accusations of domestic crimes against domestic citizens.

## III. THE PANOPTICAL FRAMEWORK

The panoptical society restricts individual autonomy by "unnecessarily constraining individual decision-making" [110] through the constant threat of visibility leveraging the inherently unbalanced power dynamic favoring governmental actors. The post-modern philosophical ombudsman Michel Foucault theorized upon this effect using Jeremy Bentham's "panopticon"--an anonymous, omniscient presence in prison architecture. [111] This panopticon establishes a regime of surveillance that through "discipline and punishment" oppresses individuals, as well as robs them of their rights to self-expression.

What then does it amount to when this society of surveillance becomes the norm? [112] Foucault sees the concept of "discipline" as "a type of power, a modality of its exercise ... a 'physics' or an 'anatomy' or power, a technology" in and of itself. [113]

This discipline becomes "nothing more than an infra-law ... law to the infinitesimal level of individual lives." [114] The "punishment" structure provided by the government disappears and becomes the mere constant fact of surveillance. [115] Knowing that one's daily communications are not private, but public, open to warrantless observation by the government and extralegally by individuals, the citizen's behavior is modified to comply accordingly. [116] A citizen, under this surveillance regime, may therefore self-censor her behavior to avoid punishment. [117] Freedom of speech is thusly nullified.

Hannah Arendt wrote on the power of violence being the unbalance of authority, with the power being in the imposing force, as the nature of violence in society. [118] This power imbalance inherits the characteristics of violence due to the unbalanced nature of power in this relationship. [119] Thus, not only is the panoptical framework established by Foucault oppressive, and a violation of an individual's rights, but it is also an act of violence against the people a government is established to protect. [120]

Reflecting upon the case law and statutes discussed, it is as if the government has conceded that the expectation of privacy exists in the home, land-line telephones, and first class mail, knowing full-well that in this age much communication occurs electronically. Yet Bentham's unverifiable omniscience, without the aspect of the public knowing of the visibility of their communications, betrayed more insidiously and pervasively the public's perceptions of privacy. [121] Citizens also lack the anxiety of the observation, underscoring the betrayal of their perceived rights and expectations. [122] Through this betrayal, the government more deeply perfects the exercise of its power. [123]

 

Rights are protected, as case law and statutes have established, though in the sense that the public is not provided the generalized power to center itself in the panopticon. [124] But once the public is apprised of its power to observe in its own extralegal methods, the panoptical prison shifts. [125] Hence, everyone may be a discipliner while constantly being open to discipline. [126] This panoptical society is one that individuals should strive to defeat so that they may live in freedom according to the rights afforded to them by customary life, codified in the U.S. Constitution.

## IV. METHODS OF PANOPTICAL PROPHYLAXIS

With the courts and Congress offering little protection for personal e-mail, and with the threat of a panoptical society on the horizon, individuals may be forced to adopt extralegal methods of protecting their perceived expectations of privacy. Fortunately, a number of technological innovations offer a variety of methods of prophylaxis from government intrusion. Through methods of encryption, individuals may practically--though perhaps not legally--conceal the contents of their e-mails from warrantless searches and seizure. Furthermore, through methods of anonymization and distributed identities, individuals may be able to thwart governmental attribution of behavior or content to their private persons. Alternative methods of communication ask the user to enter into virtual realms, unregulated by traditional law and jurisdiction. Each of these will be examined in light of current legal thought and as thought-experiments as to their relevance in protecting the public perception of privacy over electronic communications.

### A. *Encryption*

Society expects a certain level of privacy over their personal e-mail communications. Yet, Congress and the courts choose not to recognize this expectation. Thus, citizens may resort to extralegal methods of protecting their expectation of privacy. These extralegal, technological protections largely come in the form of encryption, anonymization, and using alternative methods of communication. Encryption is most commonly in the form of Pretty Good Privacy ("PGP") and SSL-type encryption of communications.

#### 1. PGP

Phil Zimmermann released a cryptography tool, dubbed Pretty Good Privacy, or "PGP," in 1991. [127] The source code and applications implementing PGP, such as GNU Privacy Guard, are freely downloadable on the Internet. [128] PGP uses public-key cryptography, a technique that sends encrypted data to a particular receiver who then must be authenticated to be able to decrypt the data. PGP uses a system of "keys" which both authenticate two parties in a communication as well as encrypt the code making it unreadable to any third party. The encryption portion of the PGP scheme alone translates messages into an "unreadable code of numbers and symbols." [129] Typical PGP usage implements at least a 128-bit key length, which on estimate would take a supercomputer "several million years" to decrypt. [130]

Prof. Orin Kerr has written extensively on the issue of encryption and Fourth Amendment protections. Kerr argues, "[E]ncryption cannot create Fourth Amendment protection because the Fourth Amendment regulates government access to communications, not the cognitive understanding of communications already obtained." [131] Yet, he says, "Few, if any, would argue the unreasonableness of a privacy expectation in this kind of Internet communication because strong encryption makes e-mail practically impossible to decrypt and virtually pointless to intercept." [132]

#### 2. Hushmail

Hushmail is a web-based and desktop application e-mail service, created by Cliff Baltzley, and now served by Hush Communcations Ltd. [133] Hushmail implements PGP encryption in the storage of e-mail written through its applications. When sending e-mail to another user of Hushmail, the e-mails are encrypted and verified using PGP's key-based authentication scheme.

Because Hushmail is operated by a business, the protections may be usurped by the business records exception

 

to the ECPA. But, it also might have judicial protection from cases such as *Long*, where the terms of service are clear in their meaning and practice to protect the privacy of its users.

### B. *Anonymization and Distributed Identity*

Anonymization may be achieved through anonymous routing of Internet data or through the use of non-traceable aliases. The former creates a "distributed identity," or one that cannot be traced to the original source through methods of re-routing the traffic information of data. The latter attempts to conceal the true identity of an individual through the use of e-mail aliases, created without divulging traceable personal details, such as one's true name, address, telephone number, etc.

#### 1. Tor

Tor is an implementation of onion-routing that provides anonymity in Internet communication. [134] Onion-routing routes encrypted Internet data through a number of verified server nodes in a network of computers where each server only "knows" the server immediately previous to it in the course of transit. In this manner, if one server is "seized" one may only be able to identify the last server the data was transmitted from. Furthermore, at each node, the data is re-encrypted and sent to a number of different nodes. Eventually, the data is collected, re-compiled, and decrypted at the originating source.

An interceptor may be able to work his way down the line of servers, but the number of nodes that one must follow will thwart this and the vast number of encryptions performed throughout. [135] While this scheme is not perfectly anonymous, it does provide a strong degree of "unlinkability" that, again, is nearly impossible to trace. [136] It must be noted that the first "hop" from the personal computer to the first router on the network is often "open" and data transmitted between the two may not be anonymous. This first hop may be protected through use of the "https" secured protocol and the data will be encrypted upon transmission. Also, use of an SSH-based SOCKS proxy to a remote proxy server running Tor will ensure encryption and anonymity of data transmission, so long as the web browser is configured such that DNS requests are also sent through the SSH tunnel. [137]

#### 2. Anonymity Via Aliases

The use of anonymous aliases erects further walls against traceability of e-mail communications. For example, one may create a free web-based e-mail account and not divulge any personal information. E-mails sent from this anonymous account may not be traceable to the true identity of the sender.

In fact, courts recognize that at least the use of an alias "does not necessarily mean that an individual does not have a reasonable expectation of privacy." [138] In *United States v. Pitts*, the court wrote:

> [T]here is nothing inherently wrong with a desire to remain anonymous when sending or receiving a package, and thus the expectation of privacy for a person using an alias in sending or receiving mail is one that society is prepared to recognize as reasonable. [139]

This reasoning may well also apply to e-mail communications. Thus it would be recommended that individuals interested in protecting their privacy rights resort to using anonymized aliases in communications.

#### 3. Wireless Defenses

Wireless networks are typically, by default, "open" networks. [140] They allow any computer user with a wireless network adapter within the range of the wireless router to obtain Internet access on the network owner's Internet bandwidth. In light of *Bartnicki* and *Stone*, electronic eavesdropping of wireless transmissions may themselves be unlawful under statute. Furthermore, individuals may use a "wireless defense" in avoiding attribution of on-line behavior to themselves. [141]

 

4. Virtual Life

The virtual world of Massively Multi-Player Online Role-Playing Games ("MMORPGs") offers a new world of socialization and communication opportunities for citizens. While the most successful MMORPG, World of Warcraft, [142] is more about Dungeons & Dragons-style battling and fantasy-based quests, Second Life is an on-line world where socialization and virtual life are the focus. In this on-line world, jurisdiction and other judicial issues have yet to be explored, much less decided. Communications sent and received in these extra-judicial realms may either be afforded "local" privacy protections or may simply be completely out of the jurisdiction of domestic courts until decided otherwise.

Currently, the accepted "state of law" on MMORPGs is laid out in the private contract terms of services agreements between the game developer and the player. There have been examples of community policing, but these "laws" only exist as long as they can be enforced. As for now, the two major issues of contention revolve around "farming" and "power-levelling," for which community policing occasionally occurs, leading to an appeal to the terms of service agreement, and if found guilty suspension of player accounts through the game developer. [143]

## V. CONCLUSION

Soon we will live in a world where virtual crimes are committed leaving only virtual trails of evidence. Where is the public vs. private in an on-line community, or an MMOPRG? [KAM2] Is there an expectation of privacy for "private" conversations on phone lines in a simulated world like Second Life or the Sims? The stage must be set properly to handle new needs in an ever-progressing world. In the virtual world, perhaps the best precedents must be set to protect privacy under the Fourth Amendment in the real world.

Prof. Kerr concedes that while encryption may not provide legal protection, it does provide the real, practical protection of privacy against government intrusion. Instead, he predicts that the legislature will meet the needs of the citizenry, by restoring "the protections we would like when the Fourth Amendment falters." The ECPA, FISA, and THE PATRIOT ACT demonstrate, however, that the legislature continues to constrict the realm of personal privacy protections. Hence, individuals must continue to seek and implement extralegal methods to protect their privacy until courts and Congress agree to accept these societal needs to avoid the oppression of the panoptical society.

[1]. B.A., Sociology, Williams College; Ed.M., International Education Policy, Harvard University; J.D. Candidate, 2008, Boston College Law School. The author extends his thanks to Catherine, Felix, and Ruki Ham for their support, advice, and wisdom, as well as Prof. Anthony Farley for the opportunity to produce this work.

[2]. *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1572 (2004).

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

[4]. *See, e.g.*, Stephen E. Henderson, *Nothing New Under the Sun? A Technological Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 522 (2005) (citing Bartnicki v. Vopper, 532 U.S. 514, 541 (2001)); *see also* Tara McGraw Swaminatha, Thinkpiece, *The Fourth Amendment Unplugged: Electronic Evidence Issues & Wireless Defenses*, 7 Yale J. L. & Tech. 51 (2004/2005) ("As a new type of technology become [sic] inextricably linked with daily life, reasonable expectations of privacy are consequently redefined.").

[5]. Legal scholars debate whether this matters in the interpretation of the Constitution. Likewise, some scholars argue that many of the technological advancements still fit into historical frameworks, conceivable at the time of the framing. For example, Prof. Orin Kerr observes the similarity between modern-day encryption methods with historical encryption methods that the Framers most likely used themselves. Orin Kerr, *The Fourth Amendment in*

 

*Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"* 33 Conn. L. Rev. 503, 527-29 (2001).

[6]. *See* Mulligan, *supra* note 2, at 1572.

[7]. *See, e.g.*, Sean J. Edgett, Comment, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339 (2003).

[8]. Am. Jur. 2d *Computers and the Internet* § 22; *see also* Modern Dictionary for the Legal Profession (3d ed. 2001): *E-mail; Electronic Mail; Electronic Mail System* ("Messages sent by computer users over the Internet. The messages may contain text, pictures, audio, and computer files such as programs and word processing documents.")

[9]. *See, e.g.*, Kerr, *supra* note 5, at 532-33 (2001) (judges will find Internet-related privacy cases as "old wine in new bottles," applying physical world principles to the Internet).

[10]. *See* Katz v. United States, 389 U.S. 347, 361 (1967).

[11]. *See* Kerr, *supra* note 5, at 507.

[12]. *See id*.

[13]. *See id*. at 531.

[14]. *See, e.g.*, *Bartnicki*, 532 U.S. at 541 (Breyer, J., concurring) (Legislatures may decide to "better tailor provisions designed to encourage, for example, more effective privacy-protecting technologies.")

[15]. Mitchell Waldman, J.D., *Expectation of Privacy in Internet Communications*, 92 A.L.R.5th 15, § 1(a) (2001).

[16]. 392 U.S. 1, 16-17 (1968) (a stop and frisk of a person's outer clothing is not a "petty indignity" allowed by law).

[17]. *Katz*, 389 U.S. at 347.

[18]. United States v. Jacobsen, 466 U.S. 109, 114 (1984); *see also*, 108 Stat. 4279 (1994).

[19]. Kyllo v. United States, 553 U.S. 27 (2001).

[20]. 389 U.S. at 347.

[21]. 277 U.S. 438 (1928). (The Supreme Court decided that warrantless searches via wiretapped telephone conversations were not protected by the Fourth Amendment. Brandeis, J., in his dissent, citing Boyd v. United States, 116 U.S. 616, 630 (1886), implied that new technologies bring into existence "new conditions and purposes" to which the majority opinion may be too overbroad an application.)

[22]. *Katz*, 389 U.S. at 353.

[23]. *See id*.

[24]. *See id*. at 361. (Harlan, J., concurring.)

[25]. *See id*. at 351.

[26]. *See id*. at 351.

 

[27]. *See id*. at 352.

[28]. *Id*.

[29]. *See id*. at 351 ("[W]hat [petitioner] sought to exclude when he entered the booth was not the intruding eye--it was the uninvited ear.")

[30]. *See id*. at 358.

[31]. *See id*.

[32]. *See* Kerr, *supra* note 5, at 507.

[33]. 771 A.2d 823 (Pa.Super. 2001); *see* Waldman, *supra* note 15.

[34]. 771 A.2d at 830-31.

[35]. *Id*. at 831.

[36]. *Id*. at 826.

[37]. *Id*.

[38]. *Id*. at 827.

[39]. *Id*. at 832.

[40]. *See, e.g.*, United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004).

[41]. E-mail sent over the Internet is sent in human-readable characters as opposed to encrypted data. Although the data is technically "encrypted" into binary code, the interpretation process into human-readable characters is trivial.

[42]. *See* Mulligan, *supra* note 2 (citing ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), aff'd, 521 U.S. 884 (1997).

[43]. *See id*. at 1562-63.

[44]. *See Proetto*, 771 A.2d at 831.

[45]. *Id*.

[46]. *See* United States. v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996); *cf.* McLaren v. Microsoft Corp., 1999 WL 339015 (Tex. App. Dallas 1999) (no reasonable expectation of privacy for e-mails sent over an employer's e-mail system and stored on an employer's office computer).

AOL offers users paid access to AOL-exclusive content, as well as access to the Internet at large. The limited-access aspect of AOL's service moved the court in *Maxwell* to afford greater privacy to AOL e-mail users as e-mails sent via AOL are not necessarily broadcast across the Internet. (Note that this also brings up issues with private messaging ("PM") abilities implemented by other limited access services, akin to AOL, on bulletin boards or social networking sites such as Facebook (http://www.facebook.com/) or MySpace (http:// www.myspace.com/), both of which require user registration, login with passwords, and PMs sent only within the system and not broadcasted to the Internet at large.

 

The most popular Internet-based e-mail services are, in order of popularity, Yahoo! Mail, Microsoft's Hotmail, and Google's Gmail. *See* Brownlow, Mark, "Email and webmail user statistics," Email Marketing Reports, December 2006 (updated January 2007) at http://www.email-marketing-reports.com/metrics/email-statistics.htm (as of Feb. 2, 2007, 05:50 GMT).

[47]. *See, e.g.*, U.S.C.A. Const. Amend. 4; *Lifshitz*, 369 F.3d at 173.

[48]. *See* U.S. v. Goldsmith, 432 F. Supp. 2d 161, 172 (D.Mass. 2006).

[49]. *See* U.S.C.A. Const. Amend. 4; Guest v. Leis, 255 F.3d 325 (6th Cir. 2001) (no reasonable expectation of privacy in electronic bulletin board system); *see also* United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997) (no reasonable expectation of privacy in electronic chat room).

[50]. *See, e.g.*, *Maxwell*, 45 M.J. at 411; *see also* Google Talk, Google Talk, Can I save my Google Talk chat histories?, http:// www.google.com/talk/about.html#history (as of Nov. 29, 2006, 04:54 GMT) (the widely used browser-embedded and stand-alone chat application saves chat sessions by default).

[51]. 533 U.S. 27 (2001).

[52]. *Kyllo*, 533 U.S. at 33-34.

[53]. *See* E. Parker Lowe, *Emailer Beware: The Fourth Amendment and Electronic Mail*, 2 OKLA. J. L. & TECH. 28 (2005), PT. IV(C)(2).

[54]. *See id*. at Pt. IV(C)(2), (citing *Kyllo*, 533 U.S. at 33-34).

[55]. *Kyllo*, 533 U.S. at 34.

[56]. *See id*. at 37.

[57]. *Jacobsen*, 466 U.S. at 114.

[58]. *See id*. at 111.

[59]. *Id*.

[60]. *Id*.

[61]. *Id*. at 112.

[62]. *Id*. at 116.

[63]. *Jacobsen*, 466 U.S. at 114.

[64]. *Id*.

[65]. *Id*. at 117-18.

[66]. *Id*.

[67]. Unsecured wireless routers broadcast their connection and allow any user within the signal's range to access the router and thus access the Internet. Often, many wireless router owners and administrators password protect

 

these routers, but these often use an easily surmisable common password unless the owner proactively changes the password.

[68]. *Bartnicki*, 532 U.S. at 514.

[69]. *Id*.

[70]. *See id*. at 524-25.

[71]. *See id*. at 534.

[72]. *People v. Stone*, 463 Mich. 558, 568 (2001).

[73]. *McKamey v. Roach*, 55 F.3d 1236 (C.A.6. 1995).

[74]. *Stone*, 462 Mich. at 564.

[75]. *U.S. v. Latham*, No. 2:06-cr-379-LDG (GWF), 2007 WL 4563459 (D. Nev. Dec. 18, 2007).

[76]. *U.S. v. Carter*, No. 2:07-CR-00184-RLH-GWF, 2008 WL 623600 (D. Nev. March 6, 2008).

[77]. *Id*. at *7.

[78]. *Id*. at *12. Such willful interception of wireless Internet connection is called "war driving."

[79]. Posting of Paul Ham to BC Law IPTF Blog, How the Government Attributes Internet Traffic to a User, http://thnlnk.com/bciptf/U.S.v.Carter/053 (March 26, 2008, 1:07 EST).

[80]. *United States v. Long*, 64 M.J. 57 (2006).

[81]. *Id*. at 58.

[82]. *Id*. at 61.

[83]. The terms of use, displayed every time a user logged onto his or her office computer, stated: "This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes." *Id*. at 60.

[84]. *Id*. at 59.

[85]. *Id*. at 63.

[86]. *Long*, 64 M.J. at 63.

 

[87]. *Id*.

[88]. *Id*. at 65.

[89]. *Id*.

[90]. *Id*.

[91]. *See Id*. at 67 (Crawford, J., dissenting).

[92]. *National Economic Research Associates, Inc. (NERA) v. Evans*, 21 Mass.L.Rptr. 337, 2006 WL 2440008 (Mass. Super. 2006).

[93]. *Id*. at *4.

[94]. *Id*.

[95]. *Id*. at *5.

[96]. *Long*, 64 M.J. at 66 ("[T]here are substantial reasons why one might be equally skeptical of the credibility of the Government witnesses. The prosecution witnesses were all admitted drug users who had incentives to testify for the Government in this case. Additionally, they were all potential accomplices and the court members were instructed by the military judge that their testimony should therefore be viewed with great caution.")

[97]. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in 18 U.S.C.).

[98]. *See* Mulligan, *supra* note 2, at 1557.

[99]. Pub. L. No. 107-56, 115 Stat. 272 (2001).

[100]. 18 U.S.C. § 2501.

[101]. Nicole Cohen, Note, *Using Instant Messages as Evidence to Convict Criminals in Light of National Security: Issues of Privacy and Authentication*, 32 New Eng. J. on Crim. & Civ. Confinement 313, 336 (2006).

[102]. Mulligan, *supra* note 2, at 1564-65.

[103]. *See id*.

[104]. *See id*. at 1570.

[105]. 18 U.S.C. §§ 2701-2711 (2000 & Supp. I 2001).

[106]. Mulligan, *supra* note 2, at 1570.

[107]. *See id*. at 1571.

[108]. Relatedly, the Federal Rules of Civil Procedure have recently been amended to discuss discovery of electronic evidence. Enacted on December 1, 2006, the implications of such rules upon requiring discovery of

 

electronic evidence and required retention policies for businesses have not yet been realized. See, e.g., FRCP, Rule 16(b), http:// www.uscourts.gov/rules/EDiscovery_w_Notes.pdf (retrieved on Dec. 4, 2006).

[109]. *See* Cohen, *supra* note 91, at 338.

[110]. John Alan Farmer, *The Specter of Crypto-Anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks*, 72 FORDHAM L. REV. 725, 730 (December, 2003).

[111]. *See generally*, MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (ALAN SHERIDAN TRANS., 1979).

[112]. *See id*. at 217.

[113]. *See id*. at 215.

[114]. *See id*. at 222.

[115]. *See id*. at 224.

[116]. *See id*. at 227.

[117]. *See* Farmer, *supra* note 100, at 730.

[118]. *See generally*, HANNAH ARENDT, ON VIOLENCE (HARVEST BOOKS, 1970).

[119]. *See id*.

[120]. Consider, for the sake of a thought experiment, Bruce Schneier's response to the question, "If you've done nothing wrong, you have nothing to worry about": (1) "If I'm not doing anything wrong, then you have no cause to watch me;" (2) "Because the government gets to define what's wrong, and they keep changing the definition;" (3) "Because you might do something wrong with my information." Bruce Schneier, Response to "If you've done nothing wrong, you have nothing to worry about," http://ask.metafilter.com/mefi/39312 (June 1, 2006, 10:26 AMe PST).

[121]. *See* Foucault, *supra* note 101, at 201.

[122]. *See id*. at 202.

[123]. *See id*. at 206.

[124]. *See id*. at 207.

[125]. *See id*. at 207.

[126]. *See id*. at 209.

[127]. *See* Wikipedia, Pretty Good Privacy, http:// en.wikipedia.org/wiki/PGP (as of Sep. 29, 2006, 15:32 GMT); *see also* Kerr, *supra* note 5, at 529-532 (in-depth discussion on the difficulty of decrypting encoded electronic text).

[128]. GNU ("GNU's Not UNIX") Privacy Guard is *available at* http:// gnupg.org/.

[129]. Am. Jur. 3d *Proof of Fact* § 4.

 

[130]. Kerr, *supra* note 5, at 530.

[131]. *See id*. at 505. It must also be noted that Kerr later refers to this article as one full of "fun puzzles," and while he still believes the reasoning to be correct, amends his thoughts in a later paper. Posting of Orin Kerr, Can Encryption Create A "Reasonable Expectation of Privacy"?, to the Volokh Conspiracy to http://volokh.com/posts/1157133639.shtml (Sept. 1, 2006, 02:00 EST).

[132]. Guirguis, 8 J. Tech. L. & Pol'y 135, 154 (2003).

[133]. *See* Wikipedia, Hushmail, http://en.wikipedia.org/wiki/Hushmail (as of Nov. 2, 2006, 14:27 GMT).

[134]. *See* Wikipedia, Onion (anonymity network), http:// thnlnk.com/wikipedia/Tor/Sfy (as of Sep. 27, 2006, 07:23 GMT).

[135]. Note, once more, Prof. Kerr's observation that a typical encryption strength at the least requires one supercomputer an estimated millions of years to decrypt a single Internet communication.

[136]. *See* Wikipedia, Onion Routing, *supra* note 124.

[137]. *See* Lifehacker, Geek to Live: Encrypt your web browsing session (with an SSH SOCKS proxy), http:// thnlnk.com/lifehacker/Encrypt.your.web.browsing.session/799 (as of March 17, 2007, 23:39 GMT).

[138]. *Goldsmith*, 432 F. Supp. 2d at 172.

[139]. United States v. Pitt, 322 F.3d 449, 459 (5th Cir. 2003).

[140]. *See* Swaminatha, *supra* note 4, at Pt. IIIA.

[141]. *See id*.

[142]. World of Warcraft is developed and published by Blizzard Entertainment. It has a subscriber base of over 7.5 million players world-wide. Wikipedia, World of Warcraft, http://en.wikipedia.org/wiki/World_of_Warcraft (as of Dec. 2, 2006, 15:59 GMT).

Second Life, developed and published by Linden Lab, has a subscriber base of over 1 million users. Wikipedia, Second Life, http:// en.wikipedia.org/wiki/Second_Life (as of Dec. 2, 2006, 15:31 GMT).

[143]. "Farming" occurs when a player, usually an individual within a business "farm," plays solely to obtain virtual currency which the farm then sells in real-world markets--and obstensibly not for the thrill of the game. "Power-levelling" is when Player A pays Player B to play A's online character until that character achieves a certain level. For example, it may one player 3 months to "level" a character to level 40 via actual game play, but they may pay another individual to spend 250 hours over two weeks to play their character to level 40 and then hand off the character to its original player.

 