WARSHAK: A TEST CASE FOR THE INTERSECTION OF LAW ENFORCEMENT AND CYBER SECURITY

Mike McNerney†

TABLE OF CONTENTS

I. Introduction. ................................................................. 345
II. The Electronic Communications Privacy Act. .......................... 347
   A. Methods for Obtaining Communications Under the Act. .......... 348
III. Warshak v. United States .................................................. 349
   A. Facts of the Case.......................................................... 349
   B. Outline of the Majority Opinion ..................................... 350
IV. Analysis............................................................................ 351
   A. Fourth Amendment Protections Should Not Apply Only Insofar as an Internet Service Provider Agreement .................................................. 351
   B. Securing Your Emails With a Password Does Not Necessarily Create a Reasonable Privacy Interest .................................................. 352
   C. Secrecy Clauses Prevent Parties From Recognizing Their Injuries........ 352
   D. Challenges to Electronic Surveillance Based on the First Amendment may Succeed Where Fourth Amendment Challenges Fail. .......... 353
   E. Defining What Exactly Constitutes a Search is Essential to Determining the Limits of Constitutional Protections. ...................... 355
V. Recommendations. ............................................................ 356
VI. Conclusion. ......................................................................... 357

I. INTRODUCTION

Countries throughout history have used technological innovations to gain an advantage on the battlefield. Whether it was the invention of iron, gunpowder, or the atomic bomb, militaries have often enlisted science to strengthen their arsenals. Sometimes these technological innovations go
beyond merely spawning new weapon systems to creating entirely new battlefields. The submarine allowed us to wage war beneath the waves using sound rather than sight. Likewise, the airplane revolutionized warfare by allowing us to attack our enemies using all three spatial dimensions with incredible speed. As recent events in Estonia and Georgia have shown, the new battlefield of this century will certainly be cyberspace. Like any new battlefield, many countries have the weapons for exploiting it but not the rules to govern it. Unlike previous battlefields, however, cyberspace is not a truly physical presence. It exists as a constantly evolving network between people rather than a geographic location within or between nations. This interpersonal network provides advantages to governments looking to secure their people but also offers complications for intelligence gathering and law enforcement. Determining the rules for operating in this virtual battlefield is therefore essential to balancing the security of nations with the freedom of their people.

Further complicating this issue is that cyber battles will not only be fought between nations. Terrorists, state, and non-state-sponsored actors, as well as criminals, inhabit this new land. Nations have to decide how they will deal with each one of these actors in times of armed conflict and in criminal investigations. In the United States specifically, our legal and intelligence communities are already finding themselves in uncharted waters with regard to cyber law. On the one hand, they need the tools to both gather intelligence and successfully prosecute criminals. On the other, people have a right to be free from unreasonable searches and the right to freedom of expression. Often times, the lines between criminal investigations and intelligence activities can become blurred. How far can a government agency go in gathering electronic information on an American citizen suspected of a crime? What implications are there for Americans suspected of terrorist activities? The American people want their government to have the tools to keep them safe, but they also want to be free from unreasonable searches and seizures. There are many difficult questions but very little settled law on the subject. Although only a small piece of the puzzle, a recent decision by the Sixth Circuit in a relatively obscure case called Warshak v. United States helps to highlight the larger national security issues that policymakers will have to face. Warshak itself ended up being dismissed on ripeness grounds, but an analysis of the decision still helps provide a framework for dealing with how the government can permissibly search the contents of electronic conversations outside of traditional means. In order to best analyze this case and the issues at hand, I will first introduce the Electronic Communications Privacy Act, which is the statute in question.

2. Warshak v. United States, 532 F.3d 521 (6th Cir. 2008).
3. Id. at 523.
4. See infra Part II (outlining the statute and expanding upon the various methods for obtaining electronic surveillance).
Next, I will introduce the case itself before outlining the majority opinion. Part IV begins the analysis and raises many of the complex issues associated with electronic surveillance and privacy. Several recommendations for courts and legislatures are included in Part V while Part VI offers a brief conclusion.

II. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The Electronic Communications Privacy Act defines “electronic communication” as any transfer of data by wire, radio, or electromagnetic system. Technically, only data temporarily passing through an electronic communication service or held as a backup by an electronic communication service can be defined as being in “electronic storage.” Electronic communications stored on a non-temporary basis do not meet this definition and are not subject to the same protections. Therefore, when it comes to emails, the protections of the Act make it a crime to intercept emails in transit and in transient electronic storage. Conversely, emails stored otherwise face little more protection than the Internet Service Provider (ISP) agrees to extend. The government may only compel the disclosure of electronic communications by an ISP held for 180 days or less pursuant to a warrant. Outside of Grand Jury subpoenas, electronic communications held for more than 180 days may be obtained by the issuance of a warrant, administrative subpoena, or court order. The requirements of this last provision, the court order, are found in § 2703(d). They state that the issuing court must be of “competent jurisdiction” and that the government must show “specific and articulable facts that there are reasonable grounds to believe that the contents of . . . [the] electronic communication[s] . . . are relevant . . . to . . . [a] criminal

5. See infra Part III (summarizing the facts of the case and providing an outline of the majority opinion in the case).
6. See infra Part IV (discussing the implications of internet privacy on current legal jurisprudence).
7. See infra Parts V (delineating the different responsibilities of the courts and legislatures in balancing security with privacy), VI.
10. See United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003) (holding that contemporaneous interception is required to implicate the Wiretap Act); but see Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 n.1 (8th Cir. 2005) (deciding that stored communications can be “electronic communications” if the case involves the continued receipt of email messages).
11. See 18 U.S.C. § 2510(15) (2006) (defining an electronic service as the means to send and receive electronic communications); United States v. Councilman, 418 F.3d 67, 77–78 (1st Cir. 2005) (finding that the purpose of the broad definition of electronic storage was to enlarge privacy protections, not to exclude email messages stored during transmission from those strong protections); see also 18 U.S.C. § 2511(4)(a) (2006) (declaring the interception of an electronic communication as punishable by fine or imprisonment); 18 U.S.C. § 2711(2) (2006) (defining a remote computing service as the “provision to the public of computer storage or processing services by means of an electronic communications system”).
13. See 18 U.S.C. § 2703(c) (2006) (delineating the circumstances under which the Government can “. . . require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer”).
investigation.” Additionally, § 2703 states that under § 2705, the government may delay disclosure for up to 90 days pursuant to a court order. Under that same section, the government may also require an ISP to disclose the existence of an investigation.

A. Methods for Obtaining Communications Under the Act

Of the three methods for obtaining electronic communications data under § 2703, the warrant is the least controversial. Searches and seizures pursuant to legally-acquired warrants are generally the constitutional norm and this provision does not seem to have ever been challenged. The second method, using an administrative subpoena or subpoena ducus tecum has long been used by agencies as part of their investigative function. However, administrative subpoenas often prove more controversial when used in a criminal investigation. Congress itself has studied amending the administrative subpoena system in order to ensure more Fourth Amendment protections. In cases of administrative subpoenas, courts usually deemed the subpoenas to be constitutional so long as: “(1) they satisfy the terms of the authorizing statute, (2) the documents requested are relevant to the investigation, (3) the information sought is not already in the government’s possession, and (4) enforcing the subpoena will not constitute an abuse of process.” To date, few if any administrative subpoenas of this nature have been challenged, so there is little settled law to study. However, there is a little more substantive law on a closely-related tool, the National Security Letter (NSL), which may provide some helpful insight. The government uses NSLs to compel private firms, such as financial institutions or telecommunications providers, to provide confidential information on their clients. While this tool has existed in some form or another for decades, the use of NSLs greatly expanded after 9/11 and the enactment of the PATRIOT Act. Incidentally, one NSL provision resided in § 2709 of the Electronic Communications Privacy Act. Civil liberties

15. Id.
18. See, e.g., Maryland v. Dyson, 527 U.S. 465, 466 (1999) (stating that the Fourth Amendment generally requires a warrant before the government may perform a search).
19. See CHARLES DOYLE, CONG. RESEARCH SERV., RS 22407, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS: A SKETCH CRS-2 (2006) (discussing that using an administrative subpoena or subpoena ducus tecum has long been an investigative tool used by agencies).
20. Id.
21. Id.
22. CHARLES DOYLE, CONG. RESEARCH SERV., RS 22122, ADMINISTRATIVE SUBPOENAS AND NATIONAL SECURITY LETTERS IN CRIMINAL AND FOREIGN INTELLIGENCE INVESTIGATIONS: BACKGROUND AND PROPOSED ADJUSTMENTS 16 (2005).
23. See id. at 20 (detailing that in 1986, Congress amended the Right to Financial Privacy Act and the Electronic Communications Privacy Act to allow the FBI to use NSLs to access customer information in certain foreign intelligence investigations).
groups have derided NSLs as a violation of privacy and an unconstitutional exercise of government power. However, given the secrecy of these NSLs and the often-accompanying gag orders, few people ever find out if an NSL has ever been used to gather personal information about them. That makes it very hard to bring a law suit to challenge NSLs because such laws can’t be challenged generally without a specific harm to the plaintiff. However, a few have managed to work their way through the judiciary system. In one case, the recently decided Doe v. Gonzales, the court decided that the gag order provisions relating to NSLs were unconstitutional and struck down the entire statute.

As stated earlier though, administrative subpoenas are not technically the same as NSLs. Additionally, the Electronic Communications Privacy Act cannot be understood as expanding the authority for such subpoenas within the framework of Warshak because the statute merely allows them to be used in situations that were previously recognized. It is rather the final method, the court order, which may most plausibly be unconstitutional and is at the center of the case. The provisions allowing for a court to issue a search order ex parte also allow notice to be withheld and do not provide for an opportunity to be heard. Such court orders raise significant privacy concerns which can strike at the heart of the Fourth Amendment. They also seem to share a lot of similarities with the controversial NSLs. As mentioned, the majority in Warshak did not decide the constitutionality of the court orders under § 2703, instead dismissing the case on ripeness grounds. However, the discussions written by both the majority and the dissent provide interesting points for discussion.

III. W ARSHAK V. UNITED STATES

A. Facts of the Case

In 2005, Warshak had become the focus of a federal criminal investigation, and the government required his ISPs to turn over his emails pursuant to two separate ex parte court orders. The issuing judge, fearing that notice of these orders would jeopardize the investigation, instructed the

---

27. Id.
29. See e.g., Doyle, supra note 22, at CRS-1 (discussing NSLs and administrative subpoenas as “closely related” but distinct tools).
31. See, e.g., Warshak, 532 F.3d at 523 (discussing the court order to obtain Warshak’s emails).
33. See Warshak, 532 F.3d at 535–37 (Martin, J., dissenting) (indicating that the constitutionality of the court order was not decided).
34. Id. at 523.
government to delay notice for 90 days.\textsuperscript{35} Warshak himself did not actually learn about the existence of these orders until a year later, when he was finally notified by the government.\textsuperscript{36} After that, he immediately filed for a preliminary injunction and sought declaratory relief to invalidate portions of the statute under the Fourth Amendment.\textsuperscript{37} In his case, “Warshak alleged that § 2703(d) violated the Fourth Amendment [both] on its face and as applied because the searches were” not based on a warrant or on sufficient probable cause.\textsuperscript{38} After winning an injunction at the district court level, the case found its way to the full Sixth Circuit court.\textsuperscript{39} Incidentally, the information gained from these activities likely helped the government to indict and convict Warshak.

\subsection*{Outline of the Majority Opinion}

In the Sixth Circuit Court decision, the majority does present several important questions despite avoiding a binding opinion on substantive legal issues. First, the court speaks of the difficulty in determining not only when and where, but also which email accounts could be searched.\textsuperscript{40} This is no small issue. As any intelligence analyst can tell you, population mobility and ready access to computer terminals make surveillance much more challenging. It used to be that the government could tap a few phone lines in order to listen to what they needed. Now, a person can access his or her email on any computer with Internet access in the world, making monitoring a person’s computer almost useless.\textsuperscript{41} To compensate, investigators must tag actual Internet and email accounts in order to ensure better surveillance.\textsuperscript{42} This means that the investigator often has access to the entire account and the information in it.\textsuperscript{43} Uncomfortable to some as it may be, this kind of surveillance has been subject to few successful lawsuits. Expectations of privacy are unclear in email accounts and some courts seem to believe that the answers often relate to ISP user agreements.\textsuperscript{44} Given that these agreements vary from ISP to ISP, the majority in \textit{Warshak} believes expectations of email privacy can only be determined on a case-by-case basis.\textsuperscript{45} Furthermore, this

\footnotesize
\begin{itemize}
  \item \textsuperscript{35} Id. at 524.
  \item \textsuperscript{36} Id.
  \item \textsuperscript{37} Id.
  \item \textsuperscript{38} Id. at 524.
  \item \textsuperscript{39} Id. at 523.
  \item \textsuperscript{40} \textit{See id.} at 526 (“Not only do ‘we [the court] have no idea whether or when’ such a search will occur but we also ‘have no idea’ what e-mail accounts, or what types of e-mail accounts, the government might investigate.” (quoting \textit{Toilet Goods Ass’n, Inc. v. Gardner}, 387 U.S. 158, 163 (1967))).
  \item \textsuperscript{41} \textit{See} Kenneth Wainstein, Assistant Attorney Gen., Nat’l Sec. Div., Dep’t of Justice, Discussion on FISA Reform Before a Meeting of the ABA Standing Committee on Law and National Security (Mar. 3, 2008), available at http://www.abanet.org/natsecurity/events.shtml (speaking on what type of reform may replace the expired temporary surveillance law and providing an overview of the issues affecting national security).
  \item \textsuperscript{42} \textit{See id.} (discussing surveillance of “foreign to foreign” email communications).
  \item \textsuperscript{43} Id.
  \item \textsuperscript{44} \textit{See, e.g., Warshak}, 532 F.3d at 526–27 (noting that a computer user’s expectation of email privacy may depend on his particular ISP user agreement).
  \item \textsuperscript{45} \textit{See id.} at 528 (“[T]his case presents a legal question that may be answered differently in different
particular court believes that the limitless range of the Fourth Amendment means that it generally should only be applied after the facts of a particular case unfold.\textsuperscript{46}

IV. ANALYSIS

A. Fourth Amendment Protections Should Not Apply Only Insofar as an Internet Service Provider Agreement

Practically speaking, adjudicating cases such as these on a case-by-case basis isn’t very satisfying. Outside of basic subscriber information, it seems hard to believe that the Fourth Amendment should only apply in so far as an ISP user agreement.\textsuperscript{47} Intuitively, changing two words in a 10,000-word document that few read or comprehend shouldn’t obliterate a person’s expectation of privacy, especially if that person still uses a private Internet account with password entry. That being said, there are some cases where a person’s lack of Internet privacy has risen to some minimal level of public consciousness so as to lessen the expectation of privacy.\textsuperscript{48} One example is with public accounts where users are often well-informed that monitoring and archival activities will take place.\textsuperscript{49} These public computers and accounts are owned by the government and not private entities so privacy expectations are probably lower.\textsuperscript{50} Another example might be with a Google email or “Gmail” account. The dynamic is somewhat different with Gmail accounts because the ISP has made it publically known that it will provide a person’s electronic information to advertisers in exchange for free email services.\textsuperscript{51} Obvioulsy, overtly handing over a subscriber’s email contents to a third party reduces the expectation of privacy. The proliferation of these types of accounts may provide the most difficulty for courts no matter what may be their philosophy because of the mix of privacy with publicity. It also shows that broad policies can be just as problematic under the current laws as deciding issues on a case-by-case basis. Courts cannot just say that all content held in email accounts are private because some is clearly not. On the other hand, broadly saying that all

\textsuperscript{46} See id. (describing the scope of the Fourth Amendment and how the Fourth Amendment was designed to account for unpredictable circumstances, which means it should be applied after these circumstances occur).

\textsuperscript{47} See United States v. Miller, 425 U.S. 435, 440 (1976) (finding that a person has no expectation of privacy in bank records because they were business records of the bank); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (noting that no court has held that subscriber information provided to an ISP is protected by the Fourth Amendment).

\textsuperscript{48} See United States v. Thorn, 375 F.3d 679, 683 (8th Cir. 2004) (deciding that a public agency’s computer-use policy precluded any reasonable expectation of privacy, cert. granted and judgment vacated on other grounds, 543 U.S. 1112 (2005)).

\textsuperscript{49} See id. (holding that a government employee had no expectation of privacy because he was completely aware of the computer-use policy that stated that the Department of Social Services had the right to access all of the agency’s computers to audit their use).

\textsuperscript{50} Id.

content in email accounts is not private destroys the right to privacy in a major form of communication.\textsuperscript{52} Perhaps a person’s ISP user agreement would affect his or her expectation of privacy if there were no passwords or if the account was shared. Alternatively, maybe the ISP should send periodic emails reiterating that a user’s account is subject to continuous and secretive monitoring by the government. Neither one of these solutions seems to be a good standard on which to base Fourth Amendment protections.

B. **Securing Your Emails With A Password Does Not Necessarily Create a Reasonable Privacy Interest**

Furthermore, the fact that a person has a password or encryption is not the end-all, be-all of privacy either. When most people think of encryption, they think of putting a lock on their information, just like one might lock the door to a safe. Clearly, people have an expectation of privacy in a locked safe, so they should also have an expectation of privacy in encrypted emails, right? Well, maybe not. If the Internet is a public domain, then sending an email through it means that you’re putting it out into the public. This is vastly different than putting your information in a locked safe on private property. So emails should receive the same level of protection as a “snail mail” letter or package then? Perhaps not. Letters and packages are usually encased in a protective cover that nominally prevents unauthorized exposure to the information inside. Emails, on the other hand, have no such physically protective enclosure. An encrypted email may be more like a shredded document that has been placed in the trash. It’s clearly settled law that the police can take that trash and, if they can put the strips back together, they can have the information as well.\textsuperscript{53} Courts seem to focus on physical security when discussing privacy, but have not really ruled on the email security much.\textsuperscript{54} More than a few problems would be solved if courts decided emails were more like sealed envelopes in the mail or shredded paper in the trash. As it stands now, an email which is encoded and sent through the public domain may only be private to the extent that the government cannot decipher it. A better understanding of where emails in general, and encrypted emails in specific, fall is essential to properly protecting privacy while balancing government power.

C. **Secrecy Clauses Prevent Parties From Recognizing Their Injuries**

Internet Service Provider User Agreements and encryption do not complete the calculus either. As the dissent in *Warshak* notes, there is a strong probability that the focus of an *ex parte* court order will never learn of the

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{52} See, e.g., id. (explaining what information Gmail gathers on its users and how it uses that information).
\item \textsuperscript{53} See Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 513–517 (2001) (describing three cases in which defendants shredded or otherwise encrypted documents in unsuccessful attempts to protect their privacy).
\item \textsuperscript{54} See id. at 517–18 (arguing that courts view encryption as affecting the government’s understanding of a document rather than access to it).
\end{itemize}
\end{footnotesize}
investigation. Just as with NSLs, these court orders are issued in secret and contain provisions that preclude the government from informing the subject of its investigation. The statute itself limits secrecy to 90 days, but there seems to be little to stop the government from maintaining secrecy indefinitely. In the case of Warshak, the subject of the investigation did not find out until over a year after the issuance of the court order. The government did not face any sanctions for the delay. Limiting adjudication of alleged violations of privacy to a case-by-case basis as the majority suggests will, therefore, allow the vast majority of incidents to go unnoticed. Additionally, the government has little incentive to play fair under the current rules. However, the reality is that the Fourth Amendment was designed to prevent the government from making unreasonable searches, not to punish it for doing so on a case-by-case basis ex post facto. The majority’s decision leads straight to the conclusion that if there is no remedy, there is no right.

D. Challenges to Electronic Surveillance Based on the First Amendment may Succeed Where Fourth Amendment Challenges Fail

Secrecy provisions such as these also open the underlying statutes to First Amendment challenges. Warshak made some of these challenges in this case. He stated that the government’s actions would chill his speech because they would hinder his use of email. He also argued that continued government searches like this would harm the speech of others as well because people would use email less as it appears to be less secure. The majority seemed to entertain this notion but rejected the arguments because the defendant technically never made a First Amendment claim. Admittedly, the court probably would have tossed the case out even if Warshak had properly raised First Amendment claims earlier, but we can’t really be sure. As with gag orders, government-sponsored searches of electronic communications could be deemed to unconstitutionally “chill speech” under the First Amendment if they

55. See Warshak v. United States, 532 F.3d 521, 536 (6th Cir. 2008) (Martin, J., dissenting) (stating “The possibility that he may be the subject of another ex parte search is anything but ‘extremely remote.’”).
56. See id. at 526–28 (describing how a lack of an expectation of privacy on the part of an email user results in the government’s ability to search email accounts by contacting email providers, possibly even foregoing notification of the individual altogether).
57. Id. at 524.
58. Id. at 524–25.
59. See id. at 534 (Martin, J., dissenting) (noting that the government paid no penalty for violating the 90-day provision).
60. See id. at 529 (stating that constitutional questions are resolved correctly when analyzed on a case-by-case basis).
61. See, e.g., Mich. Dep’t of State Police v. Sitz, 496 U.S. 444, 450 (1990) (finding that the State may interfere with an individual’s Fourth Amendment interests without being reprimanded even when it has less than probable cause and no warrant, as long as the intrusion is only minimal and is justified by law enforcements purposes).
62. See Warshak, 532 F.3d at 534 (vacating the preliminary injunction and remanding the case to the District Court to dismiss Warshak’s constitutional claim).
63. Id. at 533.
64. Id.
65. Id.
prevented people from communicating. Recent opinions seem to show that courts are warming up to First Amendment challenges in a way that they have not been for Fourth Amendment challenges. In the Doe case mentioned above, the court decided that the use of NSLs under § 2709 was facially unconstitutional as both a prior restraint and content-based restraint on free speech. While it wasn’t specifically discussed in Warshak, § 2703 allows for gag orders just like § 2709 does. These gag orders might not be indefinite like § 2709, but they may still be seen as either a prior restraint because they prevent speech from occurring, or a content-based restraint because they exclude information from the public debate. In either case, these provisions might be struck down. Should the secrecy provisions of § 2703 be struck down on free speech grounds, that may very well invalidate the entire statute, just like how the court invalidated the entire § 2709 in Doe.

This would leave the government with far fewer tools in the cyber crime and security arena.

Intelligence and law enforcement tools are important because our government has to contend with security concerns in a way that it has not had to before. Terrorists, cyber criminals, weapons of mass destruction, and the Internet make providing notice dangerous. Some domestic terrorists may be subject to the rules of surveillance under Foreign Intelligence Surveillance Act (FISA), the law that governs how the government can monitor foreign agents, but what about those criminals who are a threat to national security but who are not FISA terrorists? Arms dealers, drug and human traffickers, and others may be a danger to security but beyond the scope of FISA. If such a person, especially a domestic one, were to be provided notice of government surveillance, not only would he or she change plans and patterns, but sensitive sources and methods could also be revealed. This could drive the suspect further underground and render our nation’s surveillance techniques useless.

The dissent in Warshak discusses a policy under which the government would either give the suspect notice and an opportunity to be heard or require the government to show fact-specific evidence that the suspect has no expectation of privacy. In the case of an American suspected of criminal activity, this could mean having to prove that the suspect’s ISP user agreement negates any expectation of privacy. Additionally, if the government can’t prove this using the user agreement, the government may have to show that the suspect has no expectation of privacy in criminal or terrorist communications. The latter

68. See Doe, 500 F.Supp.2d 379 at 425 (“Because the Court finds that § 2709(c) cannot be severed from the remainder of the statute, the Court finds the entirety of § 2709 unconstitutional.”).
70. See id. (limiting the scope of entities subject to surveillance essentially to foreign governments, agents, terrorists, spies, and saboteurs).
71. See Warshak v. United States, 532 F.3d 521, 537 (6th Cir. 2008) (Martin, J., dissenting) (describing the required conduct by the government as a result of the majority ruling).
could also reveal too much about surveillance capabilities.

None of this means, however, that there is no room for due process. The dissent in Warshak criticized the majority for what they considered to be a lack of notice and opportunity to be heard.\(^\text{72}\) Many view notice and opportunity to be heard as essential to fairness and openness. Providing notice allows people to not only be aware of the government’s actions but also to bring a case in court. Practically speaking though, you can’t determine if a procedure is legal if it never gets to court. As noted above, most cases of government electronic searches never make it to court because secrecy clauses prevent anybody from knowing about them. Likewise, the opportunity to be heard before a neutral decision-maker is necessary to ensure fairness under the law. It also helps ensure that the decision-maker has all of the relevant facts needed to make a good decision. Both of these are deeply-rooted in our American system of justice and heavily favored by the dissent.

### E. Defining What Exactly Constitutes a Search is Essential to Determining the Limits of Constitutional Protections

A separate but related question is whether such governmental action even constitutes a ‘search’ at all. When it comes to pen registers and trap and trace devices, the threshold for monitoring by the government is very low.\(^\text{73}\) Additionally, if the government produces adequate probable cause, then it may institute a wiretap or Title III interception for prospective electronic data.\(^\text{74}\) However, cases where this threshold is not met create a complication. If a government program were to sit on your personal account and automatically collect information from it, would that be a search? What if the program sat on a massive server and searched the electronic information that passed through? What if the computer, or program, then handed-off suspect information to a live person? Does the answer depend on what is searched and what is filtered? The Electronic Communications Privacy Act does not really deal with these issues effectively.\(^\text{75}\) However, FISA attempts to grapple with some of these questions through a three-part process that may prove instructive here.\(^\text{76}\) For a FISA search to be valid, there must first be probable cause that the target is a foreign agent (or a lone-wolf terrorist).\(^\text{77}\) Next, there must be reason to believe

\(^{72}\) Id.

\(^{73}\) See 18 U.S.C. § 2511(2)(h)(i) (2009) (implying that pen registers may be used to monitor accounts and collect non-content information); see also Pen Registers and Trap and Trace Devices, 18 U.S.C. §§ 3121–3127 (2006) (governing the use of pen registers); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that a pen register is not a search because the subscriber had voluntarily given the information to the provider).


\(^{75}\) See United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003) (grappling with a difficult issue of *expressio unius est exclusio alterius* when interpreting the legislative intent of the Electronic Communications Privacy Act).

\(^{76}\) See Wainstein, *supra* note 41 (discussing the test for validity of a FISA search).

\(^{77}\) See id. at 17:36 (explaining that for a FISA search to be valid, probable cause must be established that the target is a foreign power, rather than simply showing that there exists a legitimate foreign intelligence purpose to target that person, as was historically required).
that the target will use that particular medium.  Finally, there must be appropriate minimization procedures. These procedures can govern what is filtered, what is saved, and what is discarded. While the extent of the government’s surveillance capabilities are a closely-guarded secret, FISA basically allows the government to conduct automated searches of foreign agents subject to appropriate filtering procedures. The FISA structure provides good lessons for domestic surveillance but FISA would still face trouble in a purely domestic arena. Not only does the government still have Fourth Amendment problems for domestic searches but it would also have a targeting one. The law would have to determine whether and under what conditions the government could target the sender or receiver of a message, and which accounts. There would also have to be procedures to prevent “reverse targeting,” or the practice of gathering information on a suspect who would otherwise be protected from surveillance by targeting one of the suspect’s contacts. By listening to a person who is known to converse with the suspect frequently, the government can effectively monitor the original suspect in an end-run around the Fourth Amendment. FISA opponents often mention reverse targeting as a principle draw-back of FISA although the government denies the practice.

V. RECOMMENDATIONS

Warshak raises interesting and challenging issues dealing with electronic communications. However, these are issues that can be handled. The courts should take the reins on a few of these issues, but most need to be handled by the legislatures. Court decisions work best with broad principles and philosophies, especially when it comes to the Constitution. Courts should also be wary of interfering too much in the realm of national security, which is a province usually reserved for other branches of government. In dealing with the present issues, the courts should determine to what level of Fourth Amendment protection emails are entitled. In other words, they should decide if emails (encrypted or otherwise) are more like letters or shredded paper for purposes of the Fourth Amendment. Deciding this question will give legislatures the appropriate framework to study when devising their own laws. It’s also an appropriate question of constitutional law for the courts to consider.

Legislatures can then decide where, when, and what electronic communications can be searched and under what conditions. In this day and age, automated searches are unavoidable. Also, the fluid nature of electronic communications means that no one person or communication can easily be targeted. Computer programs need to be able to sort through large amounts of information and sniff out what is needed. Privacy, then, may have to be

78. See id. at 24:02 (discussing the “significant oversight” provided by the FISA court in reviewing targeting procedures).
79. See id. (explaining that the FISA court reviews the minimization procedures utilized by the government to protect a domestic communicant’s privacy).
protected backwards in cyber space. First the information is gathered by a computer, and then any non-relevant information is automatically deleted. Information with possible interest is then funneled down successive layers of scrutiny with deletions of irrelevant information at each step. In short, people may unfortunately have to be satisfied with stringent minimization procedures that protect the privacy rights of individual Americans. While not ideal, it is better than the current regime and still allows for law enforcement and security. Provisions like these will help determine the level of privacy a person should truly expect in their electronic communications.

Legislatures should also provide for notice and opportunity to be heard where reasonable. Americans should be able to contest the evidence against them but we must also be mindful of security concerns. The procedures mentioned above will help strike an appropriate balance. Additionally, lawmakers should avoid draconian secrecy provisions that might violate the First Amendment. If not, entire provisions may be vacated, leaving our security apparatus weaker than before. Clear guidelines will help prevent chilling America’s free speech and avoid violating the First Amendment because people will know what can and cannot be monitored. Lack of knowledge causes fear and fear chills speech. By setting clear and predictable standards on Fourth and First Amendment issues, legislatures will promote stability. This stability will go a long way to helping the American people understand how far the powers of the government extend. Legislatures must also better define the permissible targets, which accounts can be targeted for how long, and for what purpose. They must also take steps to forbid reverse targeting. Express provisions preventing reverse targeting will help to remove any temptation on the part of the investigator.

VI. CONCLUSION

Clearly our nation must evolve its understanding of privacy. If Internet privacy is indeed something worth protecting under the Fourth and First Amendments, then our government should begin to recognize it. New laws should be passed that better protect privacy while balancing the need to investigate and gather intelligence. Our courts must evolve too. Adherence to old norms of thinking about privacy and the Fourth Amendment will inevitably swing the balance too far out in favor of the government and against the people. Courts should take the time to learn, not only about this issue, but about technology and the Internet in general. Judges can’t afford to get hung-up on out-dated notions of privacy that are based solely on physical security. One of the great strengths of our common law system is that the law evolves to meet the challenges of the day. We have fought to balance the power of the government with the rights of the people many times before so the ability exists. By taking the time to make solid and legally-sounds laws now, our nation will be well-equipped to fight the cyber wars of the future without having to trample over the rights of its citizens.