DIGITAL ACCESS TO SCHOLARSHIP AT HARVARD
DASH.HARVARD.EDU

HARVARD LIBRARY
Office for Scholarly Communication

Searches and Seizures in a Networked World

Citation
Jonathan L. Zittrain, Searches and Seizures in a Networked World, 119 Harv. L. Rev. 83 (2006).

Published Version
http://www.harvardlawreview.org/media/pdf/zittrainfor05.pdf

Permanent link
http://nrs.harvard.edu/urn-3:HUL.InstRepos:10876013

Terms of Use
This article was downloaded from Harvard University's DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA

Share Your Story

The Harvard community has made this article openly available.
Please share how this access benefits you. Submit a story .

Accessibility

SEARCHES AND SEIZURES IN A NETWORKED WORLD

Jonathan Zittrain[*]

Replying to Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005).

Professor Kerr has published a thorough and careful article on the application of the Fourth Amendment to searches of computers in private hands — a treatment that has previously escaped the attentions of legal academia.[1] Such a treatment is perhaps so overdue that it has been overtaken by two phenomena: first, the emergence of an overriding concern within the United States about terrorism; and second, changes in the way people engage in and store their most private digital communications and artifacts.

The first phenomenon has foregrounded a challenge by the executive to the very notion that certain kinds of searches and seizures may be proscribed or regulated by Congress or the judiciary. The second phenomenon, grounded in the mass public availability of always-on Internet broadband, is leading to the routine entrustment of most private data to the custody of third parties — something orthogonal to a doctrinal framework in which the custodian of matter searched, rather than the person who is the real target of interest of a search, is typically the only one capable of meaningfully asserting Fourth Amendment rights to prevent a search or the use of its fruits.

Together, these phenomena make the application of the Fourth Amendment to the "standard" searches of home computers — searches that, to be sure, are still conducted regularly by national and local law enforcement — an interesting exercise that is yet overshadowed by greatly increased government hunger for private information of all sorts, both individual and aggregate, and by rapid developments in networked technology that will be used to satisfy that hunger. Perhaps most important, these factors transform Professor Kerr's view that a search occurs for Fourth Amendment purposes only when its results are exposed to human eyes: such a notion goes from unremarkably unobjectionable — police are permitted to mirror entirely a sus-

---

[*] Professor of Internet Governance and Regulation, Oxford University; Jack N. and Lillian R. Berkman Visiting Professor for Entrepreneurial Legal Studies, Harvard Law School. I thank Erin Ashwell, David Barron, Nicholas Degani, Heather Gerken, Andrew McLaughlin, Jake Mermelstein, Charles Nesson, Jacqueline Newmyer, Leah Plunkett, and Joshua Salzman for helpful suggestions.

[1] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 533 n.1 (2005).

pect's hard drive and *then* are constitutionally limited as they perform searches on the copy — to dangerous to any notion of limited government powers. Professor Kerr appreciates this as a "troublesome" result — indeed, "downright creepy" — but does not dwell upon it beyond suggesting that the copying of data might be viewed as a seizure if not a search, at least so long as it involves some physical touching or temporary "commandeering" of the machine.[2] This view should be amplified: If remote "vacuum cleaner" approaches are used to record and store potentially all Internet and telephone communications for later searching, with no Fourth Amendment barrier to the initial information-gathering activity in the field, the government will be in a position to perform comprehensive secret surveillance of the public without any structurally enforceable barrier, because it will no longer have to demand information in individual cases from third parties or intrude upon the physical premises or possessions of a search target in order to gather information of interest. The acts of intruding upon a suspect's demesnes or compelling cooperation from a third party are natural triggers for judicial process or public objection. If the government has all necessary information for a search already in its possession, then we rely only upon its self-restraint in choosing the scope and depth of otherwise unmonitorable searching. This is precisely the self-restraint that the Fourth Amendment eschews for intrusive government searches by requiring outside monitoring by disinterested magistrates — or individually exigent circumstances in which such monitoring can be bypassed.

Professor Kerr develops the idea that "[a]ny observable retrieval of information stored on a computer hard drive, no matter how minor, should be considered a distinct Fourth Amendment search,"[3] and then examines in detail how specifically warrants should be worded in framing such searches. In light of the expansion of government surveillance since the terrorist attacks of 2001, Professor Kerr's suggestion appears both right and quaint: at exactly the time he offers a thorough framework of warrants and judicial review for searching hard drives, an increasing number of searches appear to be taking place entirely outside the well-traveled path of Fourth Amendment analysis, occurring without the knowledge of the person searched and eschewing the use of prosecutors, judges, warrants, and particularity.

A government owes its citizens physical protection, and there are times when searches are called for that do not abide by the usual Fourth Amendment protections. The Fourth Amendment itself invites departures from any particular set of implementing protections, since it

---

[2] *Id.* at 560–61.

[3] *Id.* at 547–48.

simply proscribes "unreasonable" searches and seizures. Hence searches undertaken to search for a ticking time bomb, rather than to find evidence of a past crime, may be reasonable even if undertaken without a warrant. So, too, are standards lowered when housing inspectors look for safety violations or police officers frisk a suspect for weapons — instances in which special needs like immediate security trump privacy concerns.[4] Taken together, however, the current areas of expansion of surveillance appear permanent rather than exigent, and sweeping rather than focused, causing the justifications behind special needs exceptions to swamp the baseline protections established for criminal investigations. This expansion stands to remove the structural safeguards designed to forestall the abuse of power by a government that knows our secrets.

I. SHIFTS FROM PERSONAL TO NETWORKED STORAGE

The rise of always-on broadband has led to a shift toward the use of our personal computers as mere workstations, with private data stored remotely in the hands of third parties. There is little reason to think that people have — or ought to have — any less of a first-order reasonable expectation of privacy for e-mail stored on their behalf by Google and Microsoft than they would have if it were stored "locally" in personal computers after being downloaded and deleted from their e-mail service providers. The latest version of Google Desktop offers a "Search Across Computers" feature that is advertised as allowing users with multiple computers to find documents with one computer that are stored on another.[5] It accomplishes this by sending a copy of the user's documents to Google itself. While functionally networking one's own private computers would also not appear to change expectations of privacy in their contents, the placement or storage of the data in others' hands seems to render the Fourth Amendment's doctrinal protections largely irrelevant. In *SEC v. Jerry T. O'Brien, Inc.*,[6] the Supreme Court held:

> It is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities. . . . These rulings disable respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers.[7]

---

[4] *See* Terry v. Ohio, 392 U.S. 1 (1968); Camara v. Mun. Court, 387 U.S. 523 (1967).

[5] *See* Google.com, Google Desktop — About, http://desktop.google.com/about.html#privacy (last visited Feb. 14, 2006).

[6] 467 U.S. 735 (1984).

[7] *Id.* at 743.

A transition of computing habits, from storing diaries, e-mail, and documents at home to generating business records held by a dot-com, can largely moot such debates as whether the interception of e-mail in transit (whether by government or private party) should be viewed as covered by the lesser statutory protections of the Stored Communications Act or the heightened ones of the Wiretap Act,[8] since nearly all transient communication can now end up permanently and accessibly stored in the hands of third parties.

These third parties typically say that they may elect to disclose any information upon the request of the government — at least after receiving assurances by the requesting party that the information is sought to enhance the public safety.[9] Should a custodian deny a mere request for cooperation, the records might further be sought under the Stored Communications Act, which Professor Kerr has rightly described as not entirely protective of privacy.[10]

Or the holders of private records may be compelled to release them through any of a series of expanded information-gathering tools enacted by Congress in the wake of September 11. For example, a third party storing networked, sensitive personal data could be sent a secretly obtained, Federal Intelligence Security Act (FISA)-approved PATRIOT Act section 215 order, directing the production of "any tangible things (including books, records, papers, documents, and other items) for an investigation . . . to protect against international terrorism or clandestine intelligence activities."[11] The party upon whom the order is served can neither disclose nor appeal the order.[12] The fact of the search therefore is not readily known by the target of interest in the search, since the party searched — whether a library, accountant, or Internet Service Provider (ISP) — is not itself the target of interest. Probable cause is not required for the search to be ordered, and indeed the target of interest may be assumed to be an innocent party, if the party is still generating records of interest to the government in an international terrorism or counterintelligence investigation. Roughly

---

[8] *See* United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (holding that transient e-mail falls under the heightened protections of the Wiretap Act).

[9] *See, e.g.*, Google.com, Google Privacy Policy, http://www.google.com/privacypolicy.html (last visited Feb. 14, 2006) (noting that Google discloses personal information only when it has "a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, . . . (d) protect against imminent harm to the rights, property or safety of Google, its users or the public as required or permitted by law").

[10] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208–09 (2004).

[11] 50 U.S.C. § 1861(a) (Supp. II 2002).

[12] *See id.* § 1861(c)–(d).

1700 FISA applications were lodged in each of 2003 and 2004.[13] (Four were rejected each year.)

Any of these remote hosts might also be served a "national security letter" concerning the production of "envelope information." The letters are written and executed without judicial oversight, and those who receive such letters are prohibited by law from telling anyone that they received them.[14] National security letters may be used to solicit information held by particular kinds of private parties, including the records of telephone companies, financial institutions (now including such entities as pawn shops and travel agencies), and ISPs.[15] For ISPs, the sorts of information that can be sought this way are "subscriber information and toll billing records information, or electronic communication transactional records."[16] This "envelope information" is not thought to extend to the contents of e-mail, but includes such things as the "to" and "from" fields of e-mail — or perhaps the contents of Google or other search engine queries made by a subscriber, since such queries are usually embedded in the URLs visited by that subscriber. If the government has questions about the identity of a user of a particular Internet Protocol address — the standard way to uniquely label each computer on the Internet — a national security letter could be used to match that address to a subscriber name. Under section 505 of the PATRIOT Act, national security letters must meet a standard short of the probable cause standard associated with a traditional warrant: the FBI must instead assert to the private recipients of such letters that the records are sought in connection with an investigation into international terrorism.[17] Government officials are cited as indicating that more than 30,000 national security letters are issued per year.[18] Even if recipients of FISA orders or national security letters successfully press challenges to be permitted to disclose to the public that they have received such mandates,[19] there is no assurance that they will do so — indeed, many may elect to remain silent about cooperating with

---

[13] *See* Letter from William E. Moschella, Assistant Attorney Gen., to L. Ralph Mecham, Dir., Admin. Office of the U.S. Courts (Apr. 30, 2004), *available at* http://www.fas.org/irp/agency/doj/fisa/2003rept.pdf; Letter from William E. Moschella, Assistant Attorney Gen., to J. Dennis Hastert, Speaker, U.S. House of Representatives (Apr. 1, 2005), *available at* http://www.fas.org/
irp/agency/doj/fisa/2004rept.pdf.

[14] *See* 18 U.S.C. § 2709(c) (2000).

[15] *See* 12 U.S.C. § 3414(a)(5)(A), (D) (2000 & Supp. II 2002); 15 U.S.C. § 1681u (2000 & Supp. II 2002); *id.* § 1681v(a) (Supp. II 2002); 18 U.S.C. § 2709(a) (2000); 50 U.S.C. § 436 (2000).

[16] 18 U.S.C. § 2709(a).

[17] *Id.* § 2709(b) (2000 & Supp. II 2002).

[18] Barton Gellman, *The FBI's Secret Scrutiny*, WASH. POST, Nov. 6, 2005, at A1.

[19] *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004) (holding that prohibiting an ISP from communicating the fact that it received a national security letter is an impermissible prior restraint on speech).

the government under these circumstances, keeping each of these searches secret from the target.

While techniques for obtaining private communications and data that require less than probable cause are being explicitly deployed so far in the context of terrorism prevention, the movement of data from the PC to the network suggests that local law enforcement will follow: warrants served upon personal computers and their hard drives will yield less and less information since the data resides elsewhere, driving law enforcement to the networked third parties now hosting that information.

Since the protections provided by these statutory schemes for the privacy of citizens' digital communications are low compared to the default common law protections of warrants in criminal cases, it is particularly important for government searches of the sort described here to meet a basic Fourth Amendment test of reasonableness. For remotely stored data, this suggests limiting the holding of *SEC v. Jerry T. O'Brien, Inc.* to the financial records held by a broker similar to those who figured in that case, rather than deducing that all cases of third-party custody of personal information entail no Fourth Amendment protections for the person whose information is so held. This is a reasonable limit to draw if the borders of one's home no longer correlate well to the borders of one's digital private life. The ability to store nearly all one's data remotely is an important and helpful technological advance, all the more so because the data can still be made to appear to the user as if it were sitting on his or her own personal computer. But this suggests that the happenstance of where data is actually stored should not alone control the constitutional assessment of what standard the government must meet to intrude upon it.

Consider *Chapman v. United States*,[20] in which a police search of a rented house for a whiskey still was found to be a violation of the Fourth Amendment rights of the tenant whose illegally unregistered still was found — despite the fact that the landlord had consented to the search.[21] The Court properly refused to find that the right against intrusion was held only by the absentee owner of the place intruded — rather, it was held by the person who actually lived and kept his effects there. Similarly, the data we store for ourselves in servers that others own ought to be thought of as our own papers and effects in which we have a right to be secure. Government intrusion into one's personal data should face a Fourth Amendment test whatever its storage configuration — PC or network.

---

[20] 365 U.S. 610 (1961).
[21] *Id.* at 610, 615–16.

Even information stored on a personal computer may no longer require the physical access to the hard drive that Professor Kerr so meticulously documents and for which he seeks to establish boundaries. So long as the computer is networked, the government might obtain the suspect computer's IP address using any of the less formal mechanisms described above. Then, it may insist that any provider of software for that computer that supports "automatic update" deliver a special update to the computer prompting it to divulge any contents residing on the PC to the provider, which will in turn divulge them to the government.

Professor Kerr's exposure-based approach to searches seems particularly troublesome in this context. "[I]n the computer context," he writes, "there is no need to focus the 'search' inquiry on a physical action like entry; the law can look directly to exposure."[22] By exposure, Professor Kerr means "when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer."[23] Such reasoning, however, would give constitutional imprimatur to the wholesale copying of users' hard drives over the network using this technique, entailing no physical intrusion for which a warrant would be needed, and for which the copying itself would not be deemed a search until some indefinite later time when government officials chose to examine the data so copied. Users' private data — even that stored on their own PCs — could then, under this theory, be surreptitiously obtained and stored by the government, to be searched later should probable cause arise and a warrant be obtained or one of the newer terrorism-fighting tools be used — here by the government upon its own copy of hoarded citizen data. Professor Kerr evinces some concern about this prospect and explores describing such copying as a seizure if not a search.[24] Yet he rejects declaring outright that the very production of a "complete and invasive" machine copy by the government is a seizure, instead focusing on the "interference" caused by copying — interference that wanes as the ability to intrude remotely increases. He further appears to want to avoid the "seizure" label since it raises the question of how long the government can retain any copies it makes, analogous to having to return seized physical items to their original owners.[25] But this is exactly a question that ought to figure into government-induced copying of our most private data: the reasonableness of such a search ought to hinge in part on retaining such data no longer than necessary for a specific purpose. To explain that such a

---

[22] Kerr, *supra* note 1, at 551.
[23] *Id.*
[24] *Id.* at 560–61.
[25] *Id.* at 562.

question is difficult — for the odd reason that deleting files may not actually fully erase them from a particular hard drive[26] — makes it no less pressing.

The wholesale migration of private data from personal custody to that of faraway third parties should not entail a complete stripping of our Fourth Amendment interests in having that data secure from unreasonable government intrusion. The shift from local to network storage also compels skepticism of the idea that mirroring of private data by the government is not itself a search. We should avoid setting up a constitutional framework that would be silent should the government choose to clone as much private data as it can extract from any source, left to its own self-restraint not to examine its own permanently held copy of that data without obtaining a warrant.

II. MASS DATA MINING

Professor Kerr's view that a search does not take place until human eyes set upon its results may wrongly suggest that the newly revealed National Security Agency (NSA) surveillance program, which appears to rely on mass data mining, is comparatively innocuous from a Fourth Amendment perspective.

In December 2005, the *New York Times* reported that the NSA has monitored telephone and Internet communications within the United States that originated or terminated outside the United States.[27] According to government officials cited in the article, "[u]nder a presidential order signed in 2002, the intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to Al Qaeda."[28]

The Attorney General confirmed the existence of the classified program in a press conference shortly thereafter.[29] In follow-up reporting, the *Times* reported that the NSA has "reached agreements with major American telecommunications companies to gain access to some of the country's biggest 'switches' carrying phone and e-mail traffic into and out of the country" for large-scale data mining.[30] The program was

---

[26] *Id.*

[27] *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

[28] *Id.*

[29] Press Briefing, Alberto Gonzales, Attorney Gen. & General Michael Hayden, Principal Deputy Dir. for Nat'l Intelligence (Dec. 19, 2005), *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

[30] Eric Lichtblau, *Bush Defends Spy Program and Denies Misleading Public*, N.Y. TIMES, Jan. 2, 2006, at A11.

not specifically authorized by Congress — and indeed, the Attorney General conceded that it appears on its face to violate FISA.[31] He believes it is permissible nonetheless, as authorized either by the more general Authorization for the Use of Military Force legislated in the wake of the September 11 terrorist attacks, or through the inherent (and perhaps congressionally unmodifiable) power of the President to protect national security and to wage war.[32]

The parameters of the NSA surveillance program are not well understood — public knowledge is thus far built around leaks to the *New York Times* and limited statements by public officials in reaction to the leaks — but it appears to involve data mining at key points of interconnection for the global Internet, with the acquiescence of the network operators.[33] If the NSA has indeed spliced in to Internet and telephony backbones in order to perform such scanning, there would be few technical barriers to it saving all such data as it measures it, for later searching. As such databases grow, the government then essentially possesses its own stockpile of the nation's communications on which to perform searches. For the direct purposes of the NSA program, the executive might elect to search the database for communications that appear to begin or terminate overseas and that, through the search terms used, appear to involve only terrorism. However, it — or local governments, for that matter — might then obtain traditional warrants by which to search the database more broadly. If the original compilation of the database is of no Fourth Amendment moment, then the use of warrants, based upon probable cause, to search for information having to do with regular crimes might also be deemed permissible. Such searches would naturally be secret since no further intrusion upon the target or a third party (such as an ISP) is needed to execute them.

This highlights the most worrisome aspects of current government surveillance of digital space: it is undertaken entirely in secret, both as a general matter and for any specific search, and it exists in the absence of any statutory framework or judicial oversight. Professor Stuntz explains the value of a renewed focus on analogous *physical* "data mining" via group sweeps — for example, the searching of all cars near the site of a terrorist threat — and points out that such searches are naturally (and healthily) limited by the fact that large swaths of the public are noticeably burdened by them and can therefore object to them through the judicial or political processes should

---

[31] *See* Press Briefing, *supra* note 29.

[32] *Id.*

[33] *See* Lichtblau, *supra* note 30.

they become too onerous.[34] No such check is present in the digital environment; boundless searching can be done with no noticeable burden — indeed, without notice of any kind — on the parties searched. Those who believe that no search takes place until human eyes rest upon results may not worry about data mining — they may even find such searches to comprise a perfect balance of benefit for law enforcement and protection of privacy. This view relies on two misconceptions.

First, as Professor Kerr points out, there is no such thing as a "Perfect Tool" that will ferret out only evidence of, say, a terrorist plot.[35] The existence of a trove of data — for Professor Kerr's purposes, an entire hard drive; for ours, an entire network's worth of interchanges — therefore inevitably calls upon human eyes to see both innocent and not-so-innocent contents. Professor Kerr's solution to this problem is not to limit the kinds of searches that can be performed — so-called "ex ante" restrictions imposed through warrants that clearly specify what kinds of searches can be performed — but instead to consider, though not yet fully advocate, eliminating the plain view doctrine for digital searches. This would prevent more broadly conducted searches from becoming fishing expeditions for evidence of any crime once probable cause to search for a given crime had been obtained. This solution does not prevent the revelation of wholly innocent private material found in searches — it merely alters what the government can successfully prosecute should incriminating evidence be found. In the context of broad-based secret searches, Professor Stuntz also turns to limits on prosecution to avoid abuse, believing that a line can be drawn between awful crimes that are serendipitously uncovered and less severe ones that would be off limits to prosecution,[36] even as he acknowledges that the history of criminal procedure has been "transsubstantive," with constitutional limits on searches applying "equally to suspected drug dealers and suspected terrorists."[37] He also proposes limits on public disclosure of any other data retrieved through secret searches.[38] These solutions are only effective to the extent that one believes that the principal damage from unfettered government access to private data arises from unjustified (if evidence-supported) criminal prosecutions or from embarrassing public disclosures of search results. These are evils, to be sure, but they are not the only ones. The realization that every digital movement is recorded and monitored itself will

---

[34] *See* William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2163, 2165–66 (2002).

[35] Kerr, *supra* note 1, at 569–70.

[36] *See* Stuntz, *supra* note 34, at 2183–84.

[37] *See id.* at 2140.

[38] *See id.* at 2183–84.

chill private behavior, and public concern about abuse can further affect behavior even if that concern is unwarranted because the public actors are good or because they are limited by law.

This reveals a second misconception: that a democratic system cannot thrive in the long term in the absence of independent oversight of government surveillance activity. Judge Posner believes that any abuse of secret, warrantless surveillance will be readily outed by government leaks and punished by the political process — presumably either at the ballot box or through removal, impeachment, or even prosecution of implicated officials.[39] His reasoning would appear to apply equally to wholly domestic surveillance as it does to surveillance in which one party is thought to be outside the United States. This is too thin a basis on which to find the combination of new search tactics consonant with the Fourth Amendment. The Fourth Amendment hazards an answer to the question, "Who will watch the watchers?" Judge Posner's answer — whistleblowers who leak to the press — is especially inapt when a small number of people in power could perform nearly unlimited searching without the assistance of many others, circumscribing the number of potential whistleblowers even as the amount of information they can unearth is unprecedented.

III. CONCLUSION

The power of the Fourth Amendment interpretation intended by Professor Kerr for personal hard drives in the "standard" criminal context is that it involves disinterested parties from an entirely separate branch of government providing at least a cursory review of the facts and issuing warrants in the first place, whether broadly or narrowly drawn. Each search has a beginning and an end, requiring another consultation with a magistrate if it is to be relaunched later. The Fourth Amendment has been rightly construed flexibly to allow the government to conduct certain searches in exigent circumstances without consultation with a judge, and even entirely in secret — limited exceptions to a general rule, the exceptions themselves designed and regulated by judges.

A lack of oversight or adversarial process for the kinds of searches that are about to become common threatens to have the exceptions dwarf the rule. National security letters, subject to no oversight except the conscience of the branch issuing them, push this limit, and exceed it when the recipients of such letters are said to be committing a criminal act when they consult lawyers about their options. When the determination of whether a given search falls within certain secret pa-

---

[39] *See* Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31.

rameters is made by an intelligence agency shift supervisor rather than a federal judge, as part of a program that is both secret from the public and most members of Congress, and is able to search massive amounts of private data traversing a network — the Fourth Amendment has been stretched to the point of breakage. "National security" and "terrorism" are ill-defined terms,[40] and the pressures of fighting an unending war against unseen foes are too much for even the most dedicated shift supervisor or President to handle alone.

The kind of incisive analysis used to parse the right balance to apply in permitting standard police searches of hard drives must be used to determine a new balance for searching our expanding digital world. We can find a way to use new investigative opportunities to thwart very real threats, while using processes that minimize the prospects for abuse. We can understand remotely stored data as no less precious to the public merely because it has not been limited to a single personal hard drive, and require that special circumstances be shown before it can be seized by the government.

Professor Viet Dinh, a former Department of Justice official, testified that "the current threat to America's freedom comes from Al Qaeda and others who would do harm to America and her people, and not from the men and women of law enforcement who protect us from harm."[41] Concern for privacy is not, however, premised on impugning any particular law enforcement officer — indeed, officers ought to be presumed innocent of ill motive, just as a member of the public is entitled to be, secure with his or her digital papers and effects, until there is reason to suspect otherwise. The good work of law enforcement is honored by a process by which its work is observed and regulated, and by which its extraordinary tools of information gathering and its use of force are bounded. The beauty of our system of checks and balances is that, if deployed properly, it need not ask us to trade off between fear of harm from outsiders and fear of intrusion from a runaway government.

---

[40] Professor Kerr agrees, at least regarding the definition of "terrorism." Kerr, *supra* note 1, at 580–81.

[41] *America After 9/11: Freedom Preserved or Freedom Lost?: Hearing Before the S. Comm. on the Judiciary*, 108th Cong. 277 (2003) (prepared testimony of Professor Viet D. Dinh, Professor of Law, Georgetown University Law Center).