Proportionality for High-Tech Searches

Peter P. Swire*

CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (University of Chicago Press 2007).

Professor Christopher Slobogin of the Vanderbilt University Law School shows his mastery of the Fourth Amendment in *Privacy at Risk: The New Government Surveillance and the Fourth Amendment.* Slobogin argues with passion that we need a fundamental revision of Fourth Amendment jurisprudence. He begins the book by saying: "This book is about an insidious assault on our freedom and the failure of the law to respond to it." (P. ix.) The assault comes from a wave of new surveillance technologies and techniques. The failure comes from a timid Fourth Amendment jurisprudence that is allowing these techniques to spread with few limits from the courts.

Slobogin hopes to re-organize Fourth Amendment doctrine for high-technology searches around the Proportionality Principle, which focuses on the degree of intrusiveness of a government action. This book review first describes Slobogin's main findings in areas such as physical searches of the home, physical searches of persons when in public, and government access to records held by third parties. It then underscores the importance of using the proportionality literature for an emerging controversy: searches of laptop computers and other electronic devices at the border without individualized suspicion. Finally, it focuses its comments on two topics that Slobogin does not address but which are clearly relevant to his project: the growing prominence of national security searches and the well-developed literature on the Proportionality Principle and government searches in other liberal democracies.

I. SLOBOGIN'S "PRIVACY AT RISK"

The structure of Slobogin's book is straightforward. After a brief introduction, Slobogin introduces his Fourth Amendment framework, centered on the Proportionality Principle. He then examines three areas in detail: high-tech searches of the home; camera surveillance of public spaces; and surveillance of transactions through subpoenas and other means.

An implicit theme of the book is that there is a "new" government surveillance based on emerging technologies: newly powerful sensors feed data to

* C. William O'Neill Professor of Law, Moritz College of Law of the Ohio State University. My thanks to Joseph Buoni for fine research assistance.

the government; the data is stored in newly powerful computers; and computers are linked in newly powerful networks. These technological trends have occurred for many years, but legal issues based on new technology arise in new profusion since the widespread use of personal computers in the 1980s, the rise of the Internet in the 1990s, and pervasive cameras and other sensors even more recently.

In response, Slobogin proposes a framework for Fourth Amendment law premised first on the "Proportionality Principle." This principle "allows courts to modulate the cause needed to carry out physical and transaction surveillance depending on its intrusiveness." (P. 210.) This emphasis on intrusiveness is perhaps the single organizing theme of the book, and I discuss it in more detail below. Slobogin also supports what he calls the "exigency principle." This holds that, "whenever there is time to do so, even surveillance authorized on less than probable cause will be subject to *ex ante* review by someone not involved in the search." (P. 210.)

A. *Surveillance of Private Places*

Slobogin examines modern physical searches of the home. In this realm, *Kyllo v. United States*[1] is generally considered the biggest recent victory for those who support stronger Fourth Amendment protections. As readers of this journal likely know, the Supreme Court in *Kyllo* concluded that the government could not use thermal imagers to measure the warmth of a home without a probable cause warrant.[2] Privacy advocates salute *Kyllo* because of its holding of constitutional protections against a new, high-tech form of search.

Slobogin, though, "wonders whether *Kyllo* is a Pyrric victory." (P. 51.) He persuasively analyzes a key loophole in *Kyllo*, which is that a warrant was needed where the technology, such as a thermal imager, was not in "general public use." Slobogin calls this the "Wal-Mart test"—"if the item is available at Wal-Mart, it is likely to be affordable to and accessible by a large segment of the public." (P. 57.) The problem, as Slobogin persuasively explains it, is that the cutting-edge technology of one year is on the discount shelf at Wal-Mart the next (or perhaps a couple of years after that). For instance, Wal-Mart sells night-vision binoculars that purport to permit magnified night viewing "even in total darkness." (P. 57.) Police that peer into a home using such binoculars quite possibly can do so without a warrant, even after *Kyllo*.

In response, Slobogin argues that "the ubiquity of the enhancement device the police use is irrelevant." (P. 73.) Similarly, "[s]o is any inquiry into whether the details observed through enhancement could have been viewed with the naked eye

---

[1] 533 U.S. 27 (2001).

[2] *Id*. at 41.

from a lawful vantage point."[3] (P. 73.) Instead, Slobogin deploys the proportionality test, where validity of a search "would depend on the level of justification and the level of intrusion." (P. 73.) In the alternative, Slobogin would support legislation that would "ban nonconsensual, warrantless 'visual surveillance' of 'private locations.'" (P. 76.)

B. *Surveillance of Public Places*

After this discussion of surveillance of private locations, Slobogin's next two chapters address surveillance of public places. Closed-circuit television ("CCTV") cameras are already ubiquitous in the United Kingdom and may rapidly become so in the United States. The surveillance threat from CCTV increases greatly as such cameras become smaller, cheaper, more networked, equipped with zoom lenses, backed by electronic video storage and search, and more intelligent (with face recognition and other software enhancements).

For CCTV, the key precedent is *United States v. Knotts*, which found that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[4] To overcome *Knotts*, Slobogin must first explain why the Constitution applies to public surveillance and then propose how judges could actually implement such constitutional protections. For the first task, Slobogin helpfully explains the variety of constitutional sources that could apply to CCTV surveillance. Slobogin underscores what he calls the "right to public anonymity." (P. 90.) Pervasive public surveillance can undermine freedom of speech and association, such as the right to anonymous political speech in *McIntyre v. Ohio Elections Commission*,[5] or the privacy of membership lists in *NAACP v. Alabama*.[6] The Due Process Clause protects both the right to travel, such as in *Kent v. Dulles*,[7] and the right to repose and freedom from stalking, such as in state cases enjoining anti-abortion activists from videotaping people entering and leaving an abortion clinic. (P. 103.) The general right of privacy, traced to *Griswold v. Connecticut*,[8] protects personhood and what Jed Rubenfeld has argued is "the fundamental freedom not to have one's life too totally determined by a progressively more normalizing state."[9] Slobogin also develops survey evidence that pervasive CCTV surveillance is considered

---

[3] This "lawful vantage point" idea is important because of cases that allow surveillance without a warrant from low-flying aircraft, through a small hole in a wall or curtains, or through other chinks in a house's armor. *Id*. at 73.

[4] 460 U.S. 276, 281 (1983).

[5] 514 U.S. 334 (1995).

[6] 357 U.S. 449 (1958).

[7] 357 U.S. 116 (1958).

[8] 381 U.S. 479 (1965).

[9] Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 784 (1989).

highly intrusive and thus, a violation of what society actually considers a reasonable expectation of privacy.

After assembling these arguments, Slobogin writes: "Surely if CCTV implicates the First Amendment, the due process rights to movement and repose, or the general right to privacy, it ought to implicate the Fourth Amendment as well." (P. 106.) As Slobogin explains, however, the problem is that the Supreme Court has adopted two linked doctrines: (1) the assumption-of-risk doctrine, whereby individuals have assumed the risk of being surveilled when in public; and (2) the public-exposure doctrine, whereby individuals have no right to privacy when in public. (P. 108.) Slobogin responds with a call for doctrinal change: "[W]hat is misguided is not the Court's insistence on privacy as the linchpin of Fourth Amendment jurisprudence but its equation of Fourth Amendment privacy with the assumption-of-risk and public-exposure concepts." (P. 108.) The key doctrinal shift, in Slobogin's view, is to have "an analysis grounded on the Court's alternative, and arguably more fundamental, admonition that the Fourth Amendment's scope be defined according to expectations of privacy that 'society is prepared to recognize as 'reasonable.'" (P. 108.)

I have long been sympathetic to courts' giving renewed emphasis to what constitutes a "reasonable expectation of privacy" in the light of changing technology.[10] For CCTV and other public surveillance, however, I have been baffled by what role courts could usefully play. It has been difficult for me to imagine that a magistrate should issue a warrant before a camera could view a public street. More generally, it has been difficult for me to envision an administrable approach that says when a law enforcement official is allowed to take specific action to watch individuals who are in public. After all, the history of legitimate police activity has included the "cop on the beat," keeping an eye out for suspicious behavior.[11]

Slobogin responds with a different and intriguing approach, with constitutional scrutiny focused on the creation of the camera or other surveillance system. Relying on his proportionality approach to the Fourth Amendment, Slobogin argues that "courts should set minimal guidelines and monitor police decisions to ensure that such surveillance is conducted in a reasonable manner." (P. 118.) Slobogin favors a four-step set of requirements on law enforcement:

1. Justify the need for the particular camera system;
2. Develop policies for how each camera system operates;
3. Develop policies for the storage of camera records and information sharing with other entities;

---

[10] *See* Peter P. Swire, Katz *is Dead, Long Live* Katz, 102 MICH. L. REV. 904 (2004).

[11] For a discussion of how the "cop on the beat" shifts for enforcement in cyberspace, see Peter P. Swire, *No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime*, J. TELECOMM. & HIGH TECH. L. (forthcoming 2008).

4. Assure accountability to entities outside of law enforcement to comply with the first three requirements.

In my view, these four steps are entirely sensible as a matter of policy. Indeed, the steps closely track the Privacy Impact Assessments that the federal government began to use widely for new computer systems when I worked in the Clinton Administration,[12] and which were required in federal law by the E-Government Act of 2002.[13] In addition, Slobogin's attention to information sharing is similar to my support for a "due diligence" process for government information-sharing programs.[14]

Slobogin would go beyond these federal requirements in three ways, however. First, the requirements would apply to camera systems, which do not always qualify as the "computer systems" covered by the E-Government Act. Second, he would apply the four steps to state and local camera systems. Although some states have begun to do Privacy Impact Assessments for state computer systems,[15] most state and local camera systems are installed without such a process. Third, and perhaps most importantly, Slobogin would require these procedures as a matter of constitutional law rather than public policy. This position seems to admit that public surveillance does not lend itself to the traditional authorization for surveillance of each individual (such as a stop-and-frisk under *Terry v. Ohio*[16]) or of each place (such as a search warrant for a home). Instead, Slobogin essentially advocates that the Fourth Amendment apply to surveillance *systems*, with a rational bureaucratic process to ensure that the intrusiveness of the systems is matched with proportionate procedural protections. In my view, it is an intriguing thought that Privacy Impact Assessments could be required constitutionally, but that doctrinal shift is quite possibly larger than any United States court in the near future would undertake.

---

[12] The use of Privacy Impact Assessments for new computer systems became a best practice for federal agencies.

[13] E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899 (2002); *see also* E-Gov: Powering America's Future with Technology, *available at* http://www.whitehouse.gov/omb/egov/index.html.

[14] *See* Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951 (2006).

[15] In 2008, for instance, Ohio enacted H.B 46, requiring privacy impact assessments. *See* 127th General Assembly of the State of Ohio, http://www.legislature.state.oh.us/bills.cfm?ID=127_HB_46; *see also* R. STEVE EDMONDSON, OHIO OFF. INFO. TECH., PRIVACY IMPACT ASSESSMENTS (2008), http://www.oit.ohio.gov/IGD/policy/pdfs_bulletins/ITB-2008.02.pdf (implementing statutory requirements).

[16] 392 U.S. 1 (1968).

C. *Surveillance of Private Records*

Slobogin next turns to the growing surveillance of private records, observing that "subpoenas and their progeny are far more important than physical searches of homes, businesses, and effects." (P. 141.) His basic point is simple to state but complex to put into practice: "Not all recorded information warrants maximum protection from government intrusion. But much of it deserves far better protection than it receives today." (P. 169.)

Slobogin goes into some detail on the history of subpoenas. In *Boyd v. United States*,[17] the Supreme Court held under both the Fourth and Fifth Amendments that a subpoena could not compel an individual to turn over private papers.[18] The Fifth Amendment protections against self-incrimination were mostly stripped away late in the twentieth century, in cases involving, for example, tax accountant records.[19] The Fourth Amendment protections were stripped away under the so-called "third-party doctrine," which provides that a third party that holds an individual's records can provide those records to the government. Along with many other commentators, Slobogin criticizes third-party doctrine cases, such as *United States v. Miller*,[20] where the Court found no Fourth Amendment protections for financial information voluntarily conveyed by a bank depositor to a bank. Slobogin is full-throated in his criticism: "[T]he Court simply defies reality when it says that one voluntarily surrenders information to doctors, banks, schools, and phone and Internet providers." (P. 156.) Even if one accepts the "voluntary" nature of having those records available to a third party, "the *Miller* Court's second key assertion—that one thereby assumes the risk that the third party will convey it to the government—is pure judicial fiat." (P. 157.)

Slobogin's doctrinal answer is to emphasize the distinction between government access to corporate as opposed to personal records. He agrees with William Stuntz that ready government access to corporate records is needed in order to administer many health, safety, and economic regulatory regimes. Slobogin emphasizes the importance, however, of respecting the autonomy of an individual acting in a personal capacity and the importance of using the Fourth Amendment to respect that autonomy. In my view, such a distinction between commercial and individual activity is far from easy to apply, as discussed in my own writing about how current information technology is blurring the distinction between "consumers" and "producers" in consumer protection law.[21] It may be quite difficult, for instance, to determine when someone selling on eBay is acting "commercially," with easier government access to records, as opposed to "in an

---

[17] 116 U.S. 616 (1886).

[18] *Id*. at 638.

[19] Couch v. United States, 409 U.S. 322 (1973).

[20] 425 U.S 435 (1976).

[21] *See* Peter P. Swire, Consumers as Producers (May 26, 2008) (Social Science Research Network, Working Paper), *available at* http://ssrn.com/abstract=1137486.

individual or household capacity," analogous to an old-fashioned yard sale. With that said, however, Slobogin's approach has the distinct advantage of allowing the continuation of health, safety, and other desirable regulations while also protecting individuals' sensitive personal records that are increasingly held outside of the home.

To implement this constitutional doctrine, Slobogin provides a detailed proposal that would essentially create constitutional rules for what today is covered by the Electronic Communications Privacy Act. To simplify considerably, Slobogin's approach would very roughly track the categories under current statutory law but would be a notch or two stricter in many instances before the government could get access to transactional data. (P. 186.) When it comes to what he calls "envelope information"—the information about who sent or received a communication—Slobogin says he is convinced by empirical data and critiques of his earlier work that the rules should be stricter than he previously advocated. (P. 189.) Slobogin also proposes detailed, and somewhat complex, rules for data mining.

II. ASSESSING THE BOOK: THE PROPORTIONALITY PRINCIPLE AND OTHER ASPECTS

In my view, Slobogin's book largely succeeds in what it sets out to do. The book shows the author's mastery of Fourth Amendment doctrine. It is thoroughly researched and well-written, and the analysis of cases and doctrines merits the reader's confidence. I particularly like Slobogin's use of empirical surveys to inform a court's view of a "reasonable expectation of privacy." In that respect, it may be useful to draw on the history of survey evidence used in trademark litigation. In the Lanham Act and other trademark cases, the courts have often relied on consumer surveys to address issues such as whether there is a "likelihood of confusion" between two products.[22] Survey evidence in both settings can help the legal system reach a better-informed decision about the relevant facts—the views of typical or reasonable individuals in society.

In my comments on the book, I first agree with the urgency of shifting to a proportionality approach, using the current example of border searches of laptops. I then argue that Slobogin's account would be ultimately more compelling if it were located in two crucial contexts—national security searches and the large international law literature on the Proportionality Principle.

---

[22] *See, e.g.*, Daniel A. Klein, Annotation, *Admissibility and Weight of Consumer Survey in Litigation Under Trademark Opposition, Trademark Infringement, and False Designation of Origin Provisions of Lanham Act (15 U.S.C. §§ 1063, 1114, and 1125)*, 98 A.L.R. FED. 20 (1990); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 23 (1995).

A. *The Urgency of the Proportionality Test for Border Laptop Searches*

The usefulness of the Proportionality Principle is effectively illustrated by a category of search that became much more prominent in 2008—border searches by Customs and Border Protection (CBP) of laptops and other electronic devices such as Blackberries. This issue has come into sharp focus since the April 2008 decision of the Ninth Circuit Court of Appeals in *U.S. v. Arnold*.[23] That panel clearly ruled that CBP can seize a laptop computer at the border and examine its contents without any reasonable suspicion of unlawful activity.[24]

Although the Department of Homeland Security (DHS) did not provide a witness for the first congressional hearing on this issue, in June 2008, DHS subsequently articulated arguments about why it believes such suspicionless searches are appropriate. The basic argument is that the federal government has long had plenary power to do suspicionless searches at the border, so there is nothing new about searching laptops as well. The Department said: "Making full use of our search authorities with respect to items like notebooks and backpacks, while failing to do so with respect to laptops and other devices, would ensure that terrorists and criminals receive less scrutiny at our borders just as their use of technology is becoming more sophisticated."[25]

There are many reasons for objecting, as a matter of law and policy, to suspicionless border searches of laptops. I have testified in Congress about a number of such reasons. In essence, though, the point is that searches of laptop computers are more *intrusive* than traditional physical searches at the border, even the occasional decision by a border agent to copy a few pages from a journal. Consider four reasons, among others one could develop, about why laptop searches are more intrusive. First, laptop searches last longer. The search of a backpack is complete when the traveler leaves the border. For a typical laptop, the government can make a copy of the hard drive and then search every file at its leisure. Second, the scale of laptop searches is far greater. A border agent might read a page or a few pages in a physical search. The typical laptop today has eighty gigabytes of storage—many orders of magnitude more intrusive. Third, a laptop search is like searching your home in terms of what is likely contained within. Laptops today often contain family photos, medical records, finances, personal diaries, and all the other detailed records of our personal lives. Fourth, laptops quite often contain confidential and privileged information, including journalists' notes about an investigative story, trade secrets and other key business information, and much more. Lawyers' laptops quite possibly contain attorney-client privileged

---

[23] 523 F.3d 941 (9th Cir. 2008).

[24] *Id*. at 948.

[25] Jayson Ahern, Deputy Commissioner, U.S. Customs and Border Protection, Answering Questions on Border Laptop Searches (Aug. 5, 2008), http://www.dhs.gov/journal/leadership/2008/08/answering-questions-on-border-laptop.html.

information, all revealed to the government when the border search results in the copying of the hard drive.

Using traditional Fourth Amendment analysis, the Court of Appeals in *Arnold* found the case to be an easy win for the government—there is a traditional border search power, and so the government need not justify its search of a laptop computer. The court found unpersuasive the analogy to intrusive physical searches such as body cavity searches, where the Fourth Amendment does require at least reasonable suspicion even at the border.[26]

By contrast, a Fourth Amendment oriented around the Proportionality Principle would have given advocates and the court far more room to make factual arguments about the intrusiveness of a laptop search compared with the traditional suitcase or backpack search at the border. A Fourth Amendment that insisted on Slobogin's Exigency Principle also would have insisted that the Department of Homeland Security have effective policies in place in advance, before carrying out these sorts of intrusive searches. In short, the border laptop setting illustrates the usefulness of Slobogin's approach.

B. *The Incompleteness of a Fourth Amendment Approach*

Slobogin's book takes on the large task of proposing a new, integrated approach to Fourth Amendment law for high-technology searches. It may seem a bit unfair to critique such an effort for being too narrow in scope. Nonetheless, the task of the book is too narrow in two key respects.

First, Slobogin's discussion of criminal procedure law does not address the intersection with the growing phenomenon of national security searches and seizures. For wiretaps, a majority of wiretap orders occur under the Foreign Intelligence Surveillance Act (FISA) rather than under law enforcement authorities.[27] The update of FISA enacted in 2008 will continue that trend toward widespread use of national security authorities.[28] National Security Letters (NSL) are used by the government to get telephone, banking, and other records without need for recourse to a judge. Although the Justice Department said as recently as 2004 that NSLs had been used only "scores" of times, evidence came to light that instead they have been used at a rate of over thirty-thousand times per year since September 11.[29] Significant discussion of technology and civil liberties increasingly requires a discussion of both law enforcement rules, which Slobogin

---

[26] *Arnold*, 523 F.3d at 945–46.

[27] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1308 (2004).

[28] FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

[29] *Responding to the Inspector General's Findings of Improper Use of National Security Letters by the FBI: Hearing Before the Subcomm. on the Constitution of the S. Judiciary Comm.*, 110th Cong. (2007) (testimony of Peter P. Swire), *available at* http://judiciary.senate.gov/hearings/testimony.cfm?id=2679&wit_id=6286.

discusses, and national security rules, which he does not. Going forward, we will need an integration of law enforcement and national security authorities to come to any meaningful conclusions about the state of civil liberties in an era of evolving technologies.

Second, for this reader, there was a striking omission from the book. Slobogin's single biggest emphasis in the book is on the importance of the Proportionality Principle. He would like that to become the fundamental principle of Fourth Amendment jurisprudence. As discussed above, he provides intricate doctrinal recommendations for how that principle could apply to physical searches, public activities, and surveillance of private records. Slobogin fails, however, to integrate his project into the rich international literature on the Proportionality Principle. Vicki Jackson has written recently on the pervasiveness of the Proportionality Principle:

> [I]n Canada, Germany, the European Court of Human Rights, India, Ireland, South Africa, and on occasion even in the United States, courts or tribunals invoke the basic concept of proportionality not only to review the propriety of sanctions, but also to measure the legality of a wide range of government conduct through some form of means-ends analyses. In a number of countries, proportionality analysis is treated as a general principle of public law, applicable not only to constitutional law, but also to administrative and even to international law questions.[30]

In reviewing a book on the principle by Canadian David Beatty,[31] Jackson summarizes how it applies: "[A] distinguishing feature of proportionality analysis is its eschewal of doctrinal sub-categories, its commitment to returning to foundational questions of constitutional purpose in structuring analyses of challenges to government action, and its requirement that the government come forward with justifications for statutes that infringe on protected rights."[32]

This summary of the Proportionality Principle closely matches the way that Slobogin would approach issues such as CCTV surveillance: (i) eschewal of doctrinal sub-categories (Slobogin would apply Fourth Amendment protections to "public" actions); (ii) returning to foundational questions of constitutional purpose (Slobogin articulates constitutional values that justify protection of "public" actions); and (iii) a requirement that the government come forward with justifications for its actions (Slobogin would require the government to articulate policies in advance, and have review in general by judges or others who did not propose the surveillance).

---

[30] Vicki C. Jackson, *Being Proportional About Proportionality*, 21 CONST. COMMENT. 803, 804 (2004) (book review).

[31] DAVID M. BEATTY, THE ULTIMATE RULE OF LAW (2004).

[32] Jackson, *supra* note 30, at 804.

The European Union applies the Proportionality Principle to the range of issues covered by Slobogin's book. Article 8 of the European Convention on Human Rights provides:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[33]

In the past decade, the European Court of Human Rights has upheld personal rights under this Article for areas including CCTV,[34] telephone interception,[35] and secret government files.[36] It has also provided guidance on how much "law" must be provided in advance to make government surveillance lawful.[37]

In a new article, UK Professors Ian Brown and Douwe Korff emphasize that the European Court of Justice has accepted data protection as a fundamental, constitutional issue that should be applied in accordance with the jurisprudence of the European Court of Human Rights.[38] They summarize the emerging European jurisprudence, founded on the Proportionality Principle, that applies to government access to personal data.

> [The courts] require a legal basis for any collection, storage, use, analysis, disclosure/sharing of personal data for law enforcement and anti-terrorist purposes—but a vague, broad general statutory basis is not sufficient. Such processing must be based on specific legal rules relating to the particular kind of processing operation in question. These rules must be binding, and they must lay down appropriate limits on the statutory powers such as a precise description of "the kind of information that may be recorded," "the categories of people against whom surveillance measures such as gathering and keeping information may be

---

[33] European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Apr. 11, 1950, C.E.T.S. 005.

[34] Peck v. United Kingdom, 2003-I Eur. Ct. H.R. 125, 126.

[35] Amann v. Switzerland [GC], 2000-II Eur. Ct. H.R. 247, 248.

[36] Rotaru v. Romania [GC], 2000-V Eur. Ct. H.R. 111, 112.

[37] Copland v. United Kingdom, 2007 Eur. Ct. H.R. at 12.

[38] Ian Brown & Douwe Korff, *Terrorism and the Proportionality of Internet Surveillance*, EUR. J. CRIMINOLOGY (forthcoming 2009), *available at* http://ssrn.com/abstract=1261194.

> taken" and the circumstances in which such measures may be taken. Legislation must include a clearly set out procedure to be followed for the authorisation of such measures, limits on the storage of old information and on the time for which new information can be retained. It must also include explicit, detailed provision concerning the grounds on which files can be opened, the procedure to be followed for opening or accessing the files, the persons authorised to consult the files, the nature of the files and the use that may be made of the information in the files. Such rules can be set out in subsidiary rules or regulations—but in order to qualify as "law" in Convention terms, they must be published.[39]

This summary gives a sense of modern jurisprudence for government surveillance in the democracies of Europe.

The next question is what, if anything, we in the United States should learn from the extensive jurisprudence outside of the United States about the Proportionality Principle. Vicki Jackson has argued in the *Harvard Law Review* for what she calls "engagement" with foreign constitutional sources of law: "[T]he constitution's interpreters do not treat foreign or international material as binding, or as presumptively to be followed. But neither do they put on blinders that exclude foreign legal sources and experience."[40]

I find this engagement approach to be entirely sensible. European governments, regulators, courts, and citizens face many of the same law enforcement and national security issues as the United States. The recent European decisions apply constitutional principles to precisely the sorts of issues that Slobogin analyzes and that we are facing in this country—CCTV, telephone wiretaps, and sensitive personal records held in databases. Where the Europeans create legal protections, and those structures appear stable and workable, then arguments from law enforcement that they are unworkable become less persuasive.

A useful analogy is how other courts looked to opinions by Judge Cardozo and other out-of-state judges during the common-law heyday of torts and contracts in the U.S. No one considered out-of-state decisions to be binding or hierarchical authority. Nonetheless, such decisions could readily be persuasive authority—a source that a responsible judge should consult for insights into facts and legal reasoning. When Slobogin omits reference to the large literature on the Proportionality Principle, he foregoes a major persuasive argument for his proposed reworking of the Fourth Amendment. Many of his proposed solutions have persuasive precedents in the law of other democratic legal systems. An

---

[39] *Id.* at 8.

[40] Vicki C. Jackson, *Constitutional Comparisons: Convergence, Resistance, Engagement*, 119 HARV. L. REV. 109, 114 (2005).

informed consideration of the Proportionality Principle should examine those precedents.[41]

III. CONCLUSION

Christopher Slobogin has done a large public service by reconceptualizing how the Fourth Amendment should apply to high-technology searches. The emerging problems with searches of laptops at the border further exemplify the reasons to support the Proportionality Principle at the level of either constitutional or statutory law, where greater intrusiveness of government action leads to greater safeguards. The next challenge is how to integrate this impressive theory of the Fourth Amendment into the broader international debates about the Proportionality Principle, as well as to seek to unify our understanding of how legal protections should apply both to Fourth Amendment searches, covered in this book, and national security searches, which are not.

---

[41] One objection to learning from Europe on this issue is less persuasive than it might appear at first glance. The objection would be that Europe simply imposes stricter privacy rules than the United States, as shown by the E.U. Data Protection Directive that went into effect in 1998. This stricter privacy regulation has indeed long been true with respect to data held by the private sector, as I have written about at length. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC PRIVACY, AND THE EUROPEAN PRIVACY DIRECTIVE (1998). The common wisdom, however, has been that it is the United States that has a stronger libertarian view when it comes to surveillance by the government. The Europeans, by contrast, have often allowed the government greater scope to gather personal data for use in the social-welfare states of Western Europe. When it comes to issues relevant to the Fourth Amendment, then, the baseline assumption has been that the United States historically has been stricter in important respects than Europe. It is thus an especially acute criticism of current Fourth Amendment jurisprudence if individual rights protections in the U.S. fall significantly below those in Europe. This is not an instance of a generalized European preference for privacy regulation; instead, comparison with current European constitutional law shows a lack of protections under the Fourth Amendment compared with nations that historically have often been less protective than the U.S. of individual rights in this sphere.