DOI:10.1145/1562164.1562175

Paul M. Schwartz

Law and Technology
Keeping Track of Telecommunications Surveillance

The creation of a statistical index of U.S. telecommunications surveillance activities and their results will benefit both civil liberties and law enforcement.

TELECOMMUNICATIONS SURVEILLANCE RAISES complex policy and political issues. It is also a matter of great concern for the general public. Surprisingly enough, however, the phenomenon of telecommunications surveillance is poorly measured in the U.S. at present. As a result, any attempt at rational inquiry about telecommunications surveillance is hampered by the haphazard and incomplete information the U.S. government collects about its own behavior and activities.

Neither the U.S. government nor outside experts know basic facts about the level of surveillance practices. As a consequence, U.S. citizens have limited ability to decide if there is too much or too little telecommunications surveillance. It is also impossible to determine if telecommunications surveillance is increasing or decreasing, or if law enforcement is using its surveillance capacities most effectively.[4]

Ideally, it would be possible to reach conclusions about these issues by examining data about U.S. government surveillance practices and their results. As a general model, federal and state crime statistics are publicly available and criminologists pore over these databases to spot trends and determine police activities that are effective. No such database is available about the full range of telecommunications surveillance.

Congress should create one annual report card that measures and publicizes government's performance of telecommunications surveillance.

The Telecommunications Surveillance Index

Congress should create one annual report card that measures and publicizes government's performance of telecommunications surveillance. This index will replace the bits and pieces of scattered reports that different governmental entities sometimes release. Such an index will allow year-by-year comparisons of changes in the levels of government telecommunications surveillance and permit meaningful judgments about the extent of privacy invasions and the effectiveness of the activity. In this column, I describe the gap left by the reporting provisions in current statutes, which create only an incomplete and discontinuous picture of the governmental activity. The creation of an annual telecommunications surveillance index is an urgent matter, and I will conclude by discussing four issues related to this necessary task.

To understand the shortcomings of the statutes that permit U.S. telecommunications surveillance, one needs a

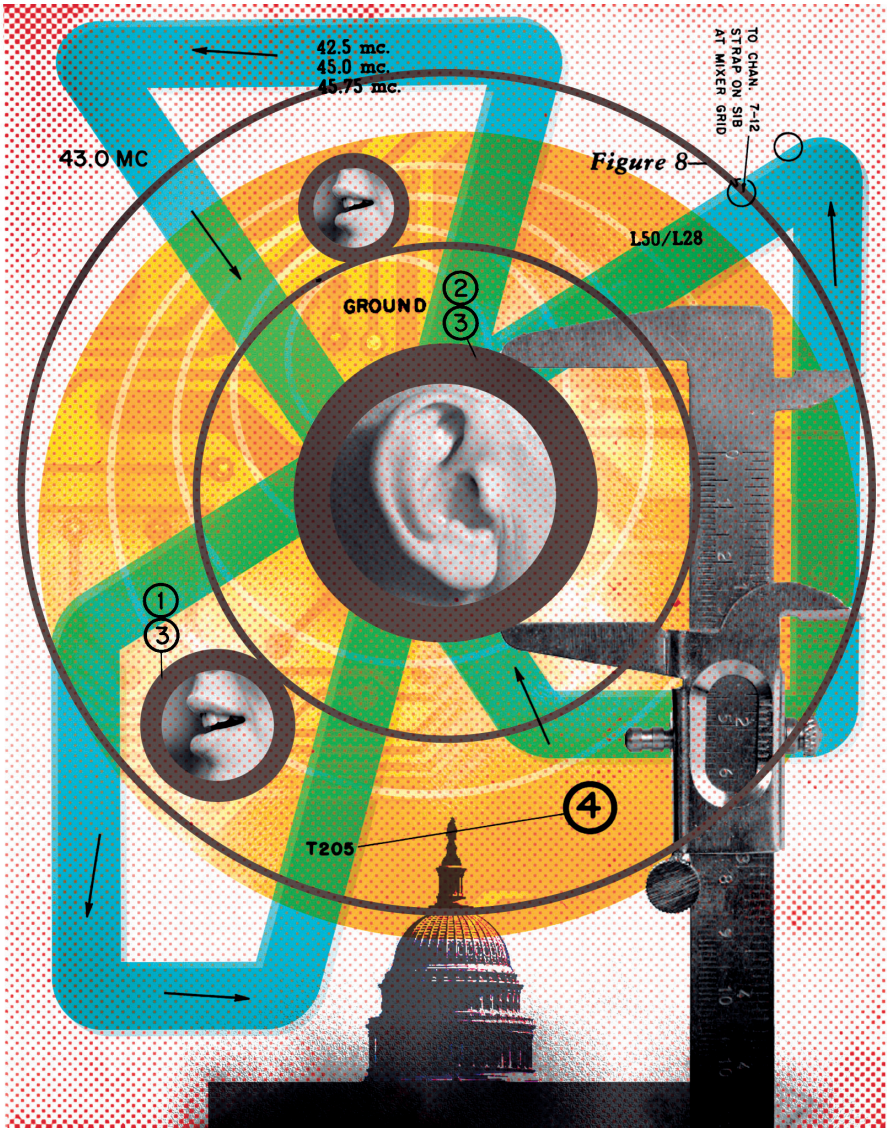
sense of how they collect information about government use. The critical statutory regulations are the Wiretap Act; the Pen Register Act; the Stored Communications Act; the Foreign Intelligence Surveillance Act (FISA); and the different provisions for National Security Letters. The first three laws concern the use of surveillance for domestic purposes—that is, in the context of ordinary criminal investigations. The last two statutes regulate the use of surveillance for foreign intelligence purposes, such as counterterrorism. And, in a nutshell, the most public information is generated about the U.S. government's use of the Wiretap Act. Yet, this law in many ways has become less important than other telecommunications surveillance statutes, and we know far less about the use of these other statutes.

Telecommunications Surveillance for Criminal Investigations

A review of the legal basis for telecommunications surveillance starts, logically, with the Wiretap Act, which is the oldest of the modern statutory authorities in this area. Enacted in 1968, the Wiretap Act sets a high statutory standard before the government can "intercept" a "wire or oral communication." It also requires the government to publish relatively detailed data sets about its use. The Wiretap Act assigns the task of collecting this information to the Administrative Office of the United States Courts, which then publishes the statistics.[1]

What is the problem then? The difficulty is that the Wiretap Act regulates only the capturing of the content of messages contemporaneously with their transmission. As an example of its coverage, if law enforcement wishes to intercept a telephone call as it is occurring, the Wiretap Act will apply. Yet, technological changes have created a variety of information that falls outside the Wiretap Act, whether because it is "telecommunications attributes" rather than content, or stored on a server. Telecommunications attributes are generally regulated by the Pen Register Act, and information stored on a server generally falls under the Stored Communications Act. I will consider each law in turn.

The Pen Register Act, as first enacted in 1986, regulated only access to telephone numbers dialed from a specific phone, or received by it. Today, the Pen Register Act, as amended by the Patriot Act in 2001, more broadly regulates access to "dialing, routing, addressing, or signaling information." Examples of such information are IP addresses and email addressing information.



Like the Wiretap Act, the Pen Register Act requires collection of information about its use. Yet, reports pursuant to it are far less detailed than those under the Wiretap Act, and the U.S. government does not make them publicly available. And perhaps the greatest surprise is that Congress has shown scant interest in even ensuring it actually receives the information to which it is statutorily entitled from the Department of Justice. Overall, the situation is reminiscent of the anarchic administrative conditions prior to the New Deal's creation of the Federal Register and other means for the orderly publication of governmental records.

As a further shortcoming, pen register reports only list *federal* collection of information pursuant to the law. If use of the Pen Register Act follows the pattern of the Wiretap Act, however, states are now engaging in far greater use of their authority than are federal law enforcement authorities.

The third statutory authority for telecommunications surveillance is the Stored Communications Act. This statute is particularly significant today because so many kinds of telecommunications occur in asynchronous fashion. For example, sending an email message may be the most prevalent

ILLUSTRATION BY STUART BRADFORD

form of telecommunications in the U.S. today. Yet, an email message is in transmission, as the term is understood under the Wiretap Act, for only a short period. Transmission is the time it takes from clicking on the "send" command to the moment the message arrives at the server of the recipient's ISP. Rather than recourse to the Wiretap Act, law enforcement typically seeks collection of email from ISPs under the Stored Communications Act, which contains requirements for obtaining access to information that are generally less rigorous than under the Wiretap Act.

Despite the centrality of the Stored Communications Act, there are almost no official statistics collected about law enforcement's use of this statute. This statute contains only a single reporting exception, which regards disclosure in an emergency. Information about its use is given to House and Senate committees, but is not made publicly available at present. In this regard, Switzerland offers a step in the right direction: in that country, the Federal Department of Justice and the police publish annual information about the number of orders for stored information.[2]

Telecommunications Surveillance for Foreign Intelligence Purposes

The three statutory authorities thus far surveyed all regulate access to telecommunications information for domestic law enforcement purposes. On the intelligence side, FISA provides the chief statutory regulation for the government's collection of information about foreign intelligence within the U.S. In addition to FISA, several statutes permit the FBI to obtain personal information from third parties through National Security Letters (NSLs). A NSL is a written directive from the FBI in cases involving national security; it does not require judicial review.

The annual index should include information about *all* statutory authorities, not just the Wiretap Act.

FISA requires the Department of Justice to file annual reports with Congress and the Administrative Office of the Courts. These reports provide merely skeletal information about the use of FISA authorities. FISA also requires the Attorney General to file reports with the Senate and House regarding all uses of pen register devices, pursuant to this statute. This information is made publicly available.

As for the NSLs, in its reauthorization of the Patriot Act in 2005, Congress required two important kinds of information to be collected about this kind of information gathering. First, it expanded an existing reporting requirement that sent information to Congress, and required annual public data on the FBI's request for NSLs. Second, the law required the Department of Justice to carry out audits of the use of NSLs. The resulting audits have already demonstrated substantial underreporting of the actual number of NSLs and misuse of statutory authorities.

Steps to Take

As I've described here, there is currently inadequate data about telecommunications surveillance in the U.S. I conclude by discussing four themes related to creation of a national telecommunications surveillance index. First, a central role should be given to the Administrative Office of the U.S. Courts, as under the Wiretap Act, in collecting and publicizing telecommunications surveillance statistics. Since 1968, the Administrative Office has successfully carried out this role pursuant to the Wiretap Act, and the other applicable statutes should be amended so that applicable information goes to this entity.

Second, the annual index should include information about *all* statutory authorities, not just the Wiretap Act. As noted earlier, this statute is less important as a source of statutory authorization for surveillance activity than the Stored Communications Act and other statutes.

Third, one of the most difficult tasks in creating an annual report card will be harmonizing the information collected within a single index. The goal is clear: to provide a picture of how activities in different statutory areas relate to each other. Nonetheless, development of a workable yardstick raises a series of complex issues because each statute sweeps in different kinds of data and, sometimes subtly, different kinds of surveillance.

Fourth, telecommunications surveillance statutes should increase independent audit functions. It is essential to have an independent assessment of the accuracy of the supplied data and the completeness of supplied reports. As part of this assessment, the use of statistical sampling of case files will be a useful technique. The Inspector General of the Department of Justice has already taken this approach in assessing use of NSLs pursuant to its audit authority. In an international illustration of this methodology, the Max Planck Institute for Foreign and International Criminal Law published an ambitious statistical analysis of a sample of telecommunications surveillance orders issued in Germany.[3]

The twin goals of an annual telecommunications surveillance index should be to minimize the impact of surveillance on civil liberties and to maximize its effectiveness for law enforcement. There is a compelling need at present for Congress to require statistical benchmarks to accompany all the laws that authorize telecommunications surveillance. C

References

1. Administrative Office of the United States Courts. *2007 Wiretap Report*; http://www.uscourts.gov/wiretap07/contents.html.
2. Eidgenössisches Justiz und Polizeidepartement, Überwachung des Post und Fernmeldeverkehrs; http://www.ejpd.admin.ch/ejpd/de/home/themen/sicherheit/ueberwachung_des_post-/statistik.html.
3. Albrecht, H.J., Grafe, A., and Kilching, M. Max-Planck-Institut fűr ausländisches und internationalises Strafrecht, Rechtswirklichkeit der Auskunftserteilung űber Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO (March 2008), Deutscher Bundestag, Drucksache 16/8434.
4. Schwartz, P.M. Reviving Telecommunications Surveillance Law. *University of Chicago Law Review 287* (2008); http://www.paulschwartz.net/pdf/12%20Schwartz%20Final%202.19.pdf.

Paul M. Schwartz is a professor of Law at the University of California, Berkeley Law School, and a director at the Berkeley Center for Law and Technology.