Speaking Out About Wiretaps

By John Podesta and Peter Swire

Friday, August 30, 2002; Page A23

Last week the Foreign Intelligence Surveillance Court, breaking 25 years of silence, released a remarkable opinion that placed limits on the way the Justice Department can conduct foreign intelligence searches on U.S. soil.

The court explained that its opinion, which the Justice Department is appealing, was needed to comply with statutes and "to protect the privacy of Americans" against "highly intrusive surveillances and searches."

Even more important, the court's opinion shows how, in each generation, we need to create new ways to bring checks and balances into our system of government.

This debate is not new. Presidents have long claimed sweeping power over foreign affairs, including the power to track foreign agents when they come into our country. In 1940 Franklin D. Roosevelt became the first president to specifically task the FBI with wiretapping and bugging suspected subversives and spies to protect the national security. With little review by Congress or the courts, the practice of warrant-less "national security" wiretaps expanded exponentially during the Cold War and over succeeding administrations of both parties.

Then, in the early 1970s, the Church Committee exposed intelligence agency abuses, including the FBI's COINTELPRO operations, which sought to disrupt political groups and discredit and harass individuals, including Martin Luther King Jr. After public debate, the CIA was barred from most investigations within the United States, and new controls were instituted to limit FBI meddling in domestic politics.

A knotty problem was how to investigate spies and other agents of foreign powers within the United States. No warrant was needed, for instance, to place a wiretap on the Soviet Embassy in Washington. The Justice Department did not need to show "probable cause" -- the usual standard for a warrant or wiretap -- before keeping tabs on a Soviet spy.

The answer to this problem was the Foreign Intelligence Surveillance Act (FISA), enacted in 1978. FISA created a "wall" between law enforcement measures aimed at criminals and foreign intelligence actions aimed at agents of a foreign power. For law enforcement, a wiretap required probable cause, and the existence of the wiretap was disclosed to the target after the fact. In addition, overreaching in a wiretap could prevent the information from being used later in a criminal trial.

By contrast, wiretaps for foreign intelligence could be placed under an easier standard. All FISA wiretap orders went to the Foreign Intelligence Surveillance Court, composed

of federal judges. The wiretaps stayed secret forever. And no evidence has ever been kept out of court because of misuse of the FISA wiretap power.

Fast-forward a generation to the attacks of last September. The wall between domestic and foreign suddenly seemed outdated to many, with terrorists clearly operating both within the United States and overseas. The Bush administration and Congress reacted by enacting the USA Patriot Act, which contained the biggest changes to FISA since its origin.

Now a FISA wiretap is permitted if a "significant" purpose is foreign intelligence, even if there is a large domestic law enforcement reason for surveillance. The standards for getting a FISA wiretap were softened, more intelligence-sharing between the FBI and the CIA was encouraged, and "roving" wiretaps were authorized to track suspects who are using multiple phones or computers to communicate.

The case for coordinating domestic and foreign intelligence is indeed strong in the face of the terrorist threat. But with the need for better coordination comes the need to create the new checks and balances appropriate a generation after FISA was enacted. Checks and balances can reduce abuses of authority, such as the pattern of misrepresentation that the court found in more than 75 FISA cases. The checks and balances also enhance performance.

One of the alarming aspects of the FISA story is that the FBI's then-secret pattern of misbehavior had so outraged the judges by summer 2001 that prosecutors were reluctant to ask for a FISA warrant to search the computer of suspected hijacker Zacarias Moussaoui. The court's opinion shows one bright line that we should retain. The court permits sharing of FISA data in some instances, but it orders that "law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution." This decision matches both the Constitution and common sense. When a prosecutor directs someone to do a search on U.S. soil, the Fourth Amendment applies and the usual warrant requirements must apply as well.

Going further, we should not leave to judges alone the need to balance foreign intelligence-gathering and constitutional liberties. Congressional oversight committees must have a better basis for seeing how surveillance laws are operating. Better oversight will lead to better laws over time, and also let the bureaucracies know that someone will hold them accountable for misrepresentations and mistakes. Senators from both parties have recently announced their frustration with the Justice Department's refusal to disclose how it is using its new powers under the USA Patriot Act.

In addition, now is the time to create a Commission on Privacy, Personal Liberty and Homeland Security as part of the bill the Senate will soon consider to create the Homeland Security Department. The USA Patriot Act was passed in haste, with no hearings on the foreign intelligence law changes. A thorough public debate is needed as the new department gears up and as the USA Patriot surveillance laws come up for reconsideration in three years.

The terrorist threat is here for the long haul. Our agents need new powers to respond to the new threats. We also need new checks and balances, tailored to those new powers.

John Podesta is a visiting professor of law at Georgetown University. Peter Swire is a professor of law at Ohio State University. They coordinated the Clinton administration's 2000 proposal to update the foreign intelligence and electronic surveillance laws.

Security and Privacy After September 11: The Health Care Example

Peter P. Swire† & Lauren B. Steinfeld††

In September 1999, the *Wall Street Journal* published a poll that asked Americans what they feared most in the upcoming century.[1] The poll included a number of frightening concerns, such as international terrorism, global warming, and world war. Ranking first among the dozen serious issues, and listed as the first or second choice of twenty-nine percent of respondents, was "erosion of personal privacy."[2] No other issue scored above twenty-three percent.[3]

Only a year later, in the wake of the September 11 attacks on the World Trade Center and the Pentagon, security issues clearly became far more important in the public mind. Although no poll has re-asked the precise question posed by the Wall Street Journal, a range of polls in the months after the attacks showed significantly greater concern about public safety and noticeably lower salience for privacy issues.[4]

As one sign of the changed times, the Bush Administration proposed new legislation, ultimately named the USA-PATRIOT Act,[5] less than a week after the attacks.[6] In the area of wiretaps and electronic surveillance, the proposal contained a number of provisions that had been previously rejected by Congress as too pro-surveillance.[7] It included other new surveillance powers that had not ever been subject

† Professor, Moritz College of Law of the Ohio State University. From March, 1999 to January, 2001 Professor Swire served as the Clinton Administration's Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that position, Professor Swire was White House coordinator for the proposed and final medical privacy rule and also chaired a White House Working Group on how to update wiretap and surveillance laws for the Internet age. He thanks Larry Glasser and Andrew Stewart for research assistance on this article. Web: http://www.osu.edu/units/law/swire.htm.

†† Chief Privacy Officer, University of Pennsylvania and Consultant, Morrison & Foerster LLP. From June, 1999 to January, 2001 Ms. Steinfeld served as the Associate Chief Counselor for Privacy, in the U.S. Office of Management and Budget. In that position, she headed a number of working groups for the medical privacy rule and worked extensively as well on numerous other privacy issues.

1. Christy Harvey, *American Opinion (A Special Report): Optimism Outduels Pessimism*, WALL ST. J., September 16, 1999, at A10.

2. *Id*.

3. *Id*.

4. *See generally* Electronic Privacy Information Center, *Public Opinion on Privacy*, *at* http://www.epic.org/privacy/survey/ (last updated Mar. 26, 2002) (collecting polling data on privacy issues).

5. Uniting and Strengthening America by Providing Appropriate Tools Required to Interpret and Obstruct Terrorism Act of 2001 (USA-PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001).

6. Bush Administration officials discussed proposals within a few days of the September 11 attacks, and the draft legislation was formally sent to Congress by Attorney General John Ashcroft by September 17. *Bush Seeks Enhanced Tools to Fight Terrorism*, CINCINNATI POST, Sept. 17, 2001, at 6A; *Bush Seeks to Expand Legal Arsenal Against Terrorism*, WALL ST. J., Sept. 18, 2001, at A24; *Congress May Loosen Bugging Restrictions*, ST. LOUIS POST-DISPATCH, Sept. 18, 2001, AT A8; *Manhunt for Accomplices Widens; Ashcroft Seeks Greater Police Powers*, GANNETT NEWS SERV., Sept. 17, 2001, *available at* 2001 WL 5112790.

7. Examples include broader powers to conduct roving wiretaps, expansion of the use of foreign intelligence surveillance wiretaps, and easier access by law enforcement to voice mail messages. *See infra*

to any hearing or debate in Congress.[8]

Just the previous summer, the Clinton Administration had proposed updating the same laws in ways that also updated law enforcement authorities while being more protective of privacy.[9] The House Judiciary Committee, with an overwhelming bipartisan majority, had amended the bill substantially further toward the privacy side.[10] Now, following the attacks, the previous legislative momentum toward greater privacy protections suddenly shifted to greater government surveillance powers than anyone would have seriously proposed a year earlier. The USA-PATRIOT Act passed on October 25, 2001.[11] Critics of the Act were able to make few amendments during its rushed consideration, although some of the most worrisome surveillance provisions will sunset in 2004.[12]

This legislative about-face in the area of surveillance law raises a linked series of questions that we address in this Article. First, we explore the relationship between protecting privacy, an especially hot issue before September 11, and protecting security, an especially hot issue since then. We do this by exploring the situations in which the two goals are antagonistic, what we call "privacy *vs.* security," and other situations in which the two goals are complementary, what we call "privacy *and* security."

A next issue to consider is the extent to which the shifting public sentiment about the relative importance of security and privacy should lead us to reexamine privacy initiatives put into place before September 11. The most far-reaching of these is the medical privacy regulation issued in 2000 under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and scheduled for compliance by health care providers, insurers, and others by April 2003.[13] In the wake of the September 11 attacks, for instance, we might wonder how well the HIPAA privacy rule allows for reporting to law enforcement officials about terrorist or other security threats. In the wake of the anthrax incidents from the fall of 2001, we might similarly wonder how well the public health reporting rules would work during a period of heightened security concern.

Fortunately, a careful inspection of the medical privacy rule shows that extensive public health and public safety protections were built into the final rule, even though it was drafted before September 11.[14] Indeed, the scope of these protections is not surprising, in light of the extensive participation of both public health and public safety

---

text accompanying notes **Error! Bookmark not defined.**-**Error! Bookmark not defined.** (discussing new powers under the USA-PATRIOT Act).

8. For example, the Act allows law enforcement to monitor telephone and e-mail communications on an ongoing basis to catch suspected computer hackers. *See* § 217, 115. Stat. at 290.

9. *See* Press Release, The White House, Assuring Security and Trust in Cyberspace, (July 17, 2000) (announcing legislation proposed by Chief of Staff John D. Podesta in remarks at the National Press Club) *available at* http://www.privacy2000.org/archives/ (last visited Apr. 5, 2002). For the text of Podesta's remarks, see Press Release, The White House, Remarks by the President's Chief of Staff John D. Podesta on Electronic Privacy to National Press Club, (July 18, 2000), *available at* http://www.privacy2000.org/archives/.

10. Press Release, The White House, Press Briefing by Chief of Staff John Podesta to Internet Press Organizations (Oct. 2, 2000) (noting a bill that improves privacy protection just passed the House Judiciary Committee, but expressing hope that the Senate would strengthen the privacy protections even further).

11. The USA-PATRIOT Act was passed by Congress on October 25, 2001 and signed by President Bush two days later. Ann McFeatters, *Bush Signs Anti-Terror Bill, Says Tough Law Will Preserve Constitutional Rights*, PITTSBURG POST-GAZETTE, Oct. 27, 2001, at A6.

12. For analyses of the USA-PATRIOT Act, see Peter P. Swire, *If Surveillance Expands, Safeguard Civil Liberties*, ATLANTA J. CONST., Oct. 21, 2001, at D2; Peter P. Swire, *Administration Wiretap Proposal Hits the Right Issues But Goes Too Far*, Oct. 3, 2001, Brookings Institution, http:// www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm (Oct. 3, 2001).

13. 45 C.F.R. § 164.534 (2001). The deadline for compliance with the rule is now April 23, 2003. *See* Office for Civil Rights, National Standards to Protect the Privacy of Personal Health Information, *at* www.hhs.gov/ocr/hipaa (date revised Mar. 27, 2002).

14. *See* discussion *infra* Part III.

officials in the drafting of the regulation. In light of these existing protections, considerable skepticism is appropriate when examining new proposals to alter public health or public safety provisions in the HIPAA privacy rule. There should be concrete showings of particular need, not broad assertions that "everything is different after September 11."

This inspection of the medical privacy rule is distinctly heartening, as is the conclusion in this Article that implementing security can provide a useful opportunity to implement privacy. The statutory call for privacy protection in HIPAA was a result of an understanding in Congress that the shift to electronic medical records required that security and privacy be built in at the same time, as part of a unified upgrading of medical information systems. To an extent not often enough realized to date, this upgrading of systems means that we more often face a situation of security *and* privacy, working together, than we might otherwise have suspected.

* *

CONCLUSION

In the days, weeks, and months after the attacks on the World Trade Center and the Pentagon, many of us have had the feeling that we wanted to "do something" to help respond to the tragedy and ensure that similar attacks do not happen again. Politicians seeking public approval and possible reelection are probably at least as prone as ordinary citizens to want to show that they are "doing something" to face the new circumstances. One understandable result was to pass new laws that demonstrate the strong, and often sincere, feelings of political leaders and the public.

The new surveillance provisions of the USA-PATRIOT Act are one example of the political response to the September 11 attacks. Time will tell us much about the desirability of the new government powers. By the time the act sunsets in 2004, we will be in a better position to assess whether the new powers are a valuable response to the new threats of a dangerous world or else an overreaction to a terrible, one-time tragedy. Between now and 2004 those of us who care about these issues have an important homework assignment. We should help the Congress to understand the strengths and weaknesses of the USA-PATRIOT surveillance provisions, and take advantage of the intervening time to have a thoughtful and informed public debate on how to achieve security and privacy in this area.

In the area of medical privacy, this Article's analysis indicates that the rule stands up well to the concerns of the post-September 11 era. Concerns about public safety are met by existing provisions that permit disclosures to protect national security, to react to emergency circumstances, and to respond to law enforcement inquiries. Concerns about public health, as suggested by the anthrax incident, are also met by the current rule. We are not aware of any needed disclosures for public health purposes that are prohibited by the medical privacy rule.

A broader message of this Article is that the protection of privacy and security is often best done together. The most effective and least costly way to protect both is to insist on doing so at the time of a computer system upgrade. For medical records, we are in the middle of a one-time shift from the mostly paper records that existed in 1990 to the mostly-electronic records that will exist by 2010. The 1996 HIPAA statute correctly required that privacy and security protections should be an integral part of this one-time shift. Health care providers and plans will assuredly shift to electronic systems when required to do so in order to qualify for payment by Medicare and other sources. There is no better time to insist on shifting to privacy and security safeguards as well.

This insight teaches a lesson as well about how state public health laws should be updated as legislatures react to the experience of the anthrax attacks. The anthrax

attacks, and the resulting public attention to public health issues, create the possibility of a once-in-a-generation overhaul of public health statutes. These state public health authorities are not generally covered by the HIPAA privacy and security requirements. If and when state legislatures move forward with new public health legislation, it is crucial to create privacy and security safeguards as an integral part of the new information systems that will handle our public health records in the future. This is the best route to achieving the privacy and security that most Americans desire and that we can achieve.