Homeland Security and the Future of Privacy Rights: A Commentary

By James T. O'Reilly

Your individual privacy is more at risk in the United States than in other countries that are also fighting terrorism. Has our Homeland Security bureaucracy failed us in protection of our privacy rights? We can expect congressional efforts in 2009 to create a European-style robust protector of privacy rights as the outgoing administration's secrecy fetishes fade away.

American interest in privacy over the past century has been inconsistent at best, with waves of action on privacy issues followed by long periods of inaction. As a result, we have an ineffective patchwork of sector-specific privacy laws and conflicting state legislation. Our nation's current focus on homeland security has created yet another wave of interest in privacy protections but, as will be seen in the following pages, this wave has the potential to remake the entire American privacy framework.

"Personal privacy" can be defined as the ability to exclude others from seeing and using personally sensitive information; "privacy" is the exclusion of others from individualized data without one's individual consent to disclose those data to those particular persons. By contrast, "secrecy" is a governmental or institutional policy to exclude as many others as possible from seeing and using personally sensitive information, making the data valuable by virtue of exclusion.

The Federal Lawyer, of course, takes no position on the political aspects of resolving the many issues Americans face, but it affords a forum for exploring the legal consequences of complex policy issues. Critics contend that loss of individual privacy rights is part of the "collateral damage" that the Bush administration has tolerated to pursue its goals. Whether the issue is the amassing of digital files, warrantless wiretaps, prisoner secrecy, novel means of telecommunications data mining, use of human biomarker indicators for screening travelers, or the search of the microfiche passport records of a presidential candidate—loss of privacy is increasingly a matter of public concern and debate.

Defenders of the administration's privacy actions often use the words "necessary," "wartime," "vital," and the like when defending searches of personal data for federal purposes. But must personal privacy *always* be the victim of security measures? Clearly, the answer is no, as evidenced by European governments, which effectively balance these interests without encroaching so greatly on their citizens' privacy rights. Can a perception of respect for individual privacy aid the U.S. government's intelligence gathering efforts? Probably so, because robust security depends not just on high-tech surveillance but also on intelligence gathered by human observers. Human intelligence comes from trusted sources, and trust is based on enlightened self-interest. Trust requires confidence, and the evasion of legal safeguards by a nation that says that it promotes the rule of law undercuts a person's trust in that nation.

The Growth of Privacy as a Public Issue

Awareness of government threats to individual privacy has increased significantly in recent years, and this is the result of three developments:

- Economic awareness of privacy is greater than ever. Consumers equate the loss of privacy with identity theft, which editors and broadcasters are eager to cover, and which makes privacy far more of a pocketbook issue for voters than it had been before.
- Globalization has made the European Union's privacy regimes and those of other international governments more visible to the average American voter.
- Media awareness has heightened with the corresponding drop in the current administration's credibility. To put it simply, justifications for secrecy for the sake of security do not fare so well in light of other administration claims with respect to homeland security that turned out to lack credibility (such as the infamous justification for the current war in Iraq—Saddam Hussein's possession of weapons of mass destruction).

History of Privacy Law

I have been studying privacy issues for 35 years. In past years it was easy to ignore privacy; it was viewed as a backwater of administrative law scholarship, with a few of us participating in quaintly idealistic and largely theoretical debates. Times have changed remarkably in recent years, by any index of public attention. Average Americans are now aware of privacy via their wallets, and we all now "get it." Thanks to ubiquitous frauds like the Nigerian Internet scams, news media coverage about government spying, breaches of personal information provided for credit card accounts, and the costs of software to ensure privacy of information sent, received, and stored on personal computers, everyone is now aware that the dynamics of the privacy debate have shifted. Lawyers who have clients in Europe, hospitals or financial institutions as clients, and the like are now confronted by privacy concerns in almost every transaction they undertake. Voters' awareness of threats to personal privacy rights has greatly expanded. The wave of interest is not abating. The history of American legislation

dealing with privacy issues shows the significance of our current situation.

The history of federal privacy law reaches back to 1890, when Harvard published Brandeis' seminal article that postulated a constitutional right to privacy.[1] Privacy law was gradually expanded as a common law tort of invasion of privacy, but legislation lagged behind court recognition of an individual's privacy rights. The most controversial line of judicial privacy cases, exemplified by *Griswold v. Connecticut* and *Roe v. Wade*, dealt with the privacy of sexual and reproductive activities.[2] The oldest federal privacy protections are found in legislation covering census reports and individual income tax returns. Unlike homeland security, we have a constitutional mandate for conducting a census and collecting income taxes, and the attendant privacy needs pervade the underpinnings of each program. Beyond these are the dozen or so significant programmatic privacy laws related to financial transactions, electronically stored health records, information about the transmission of diseases, and so forth.

The cycle of federal privacy legislation appears like a wave or a mathematical sine curve that is rising again. A democracy like ours passes legislation in cycles in response to stimuli. A wave of privacy legislation rises out of perceived abuses and crests with a foamy splash of publicity about the new legislation. The wave then is undercut and neutralized by the undertow of bureaucracy, after which it is underappreciated and underused by affected persons. The wave then recedes as it gets administratively buried in the fine print of exceptions. News media attention to that aspect of privacy fades because of the perception that the problem has been fixed. The next wave of privacy legislation comes up on a different topic, as compromise laws are passed, and again federal agencies undercut the wave as the statute is implemented in order to carry on as before despite the new statutory focus on privacy protection.

In 2008, privacy is once again rising as an issue. The public's perception of privacy rights arising from revelations of government-sponsored or -approved activities—including data mining, warrantless wiretaps, breaches of the security of private records, library checkout "national security letters," renditions, abuse of the Foreign Intelligence Surveillance Act (FISA) process, the existence of secret prisons, and other incidents stemming from the current focus on homeland security—will generate a wave of new privacy legislation in 2009 or beyond. Public attention to the inadequacies of past legislation like the failed Privacy Act of 1974[3] will increase. And the news media will probe how weak and full of holes our privacy legislation has been. Put simply, the wave is rising again.

Failures of the Privacy Act

The Privacy Act of 1974 has been a failure, repeatedly coming up short by comparison to state laws, to Canadian laws, to European laws, and the like. I say "failed" because the law's teeth were pulled out during the final stage of the legislation; therefore the legislation did not result in systematic improvements in performance by agencies engaged in law enforcement and security. While updating our encyclopedic text, *Federal Information Disclosure*,[4] I have read literally every case decided under the act as well as dozens of articles related to the act. The act offered a great concept, but it has proven to be a missed opportunity that did not deliver on Rep. Bella Abzug's (D-N.Y.) lofty goals for the legislation she introduced.

When the Privacy Act was first debated in 1973, privacy was a hot issue[5]—much like it is today. The lies and deception of the executive branch were exposed, the world was alarmed at the President's activities, wiretaps were frequently debated, denials were issued and retracted on a regular basis, and the news media used leaks to expose more and more invasions of privacy. In fall 1974, with White House Chief of Staff Dick Cheney involved, advocates for secrecy were successful in getting President Gerald R. Ford to veto expansions of the Freedom of Information Act,[6] and the administration was able to reduce the force of the new Privacy Act and steer the oversight of the new law into the friendly hands of the White House Office of Management and Budget.

The compromises embodied in the 1974 House floor amendments and Senate committee markups left the statute encumbered and its coverage limited to bureaucratic "systems of records."[7] The act was passed with broad exceptions, and its language created time-consuming formalities of requests and responses via "snail-mail." The agencies resisted implementation of the act, and the Office of Management and Budget obfuscated. In the absence of a firm mandate and a designated federal champion, privacy became just another block for bureaucrats to check off on a form.

The 1974 congressional compromises punted the most important reforms into the hands of a Privacy Protection Study Commission. All the unresolved issues raised but not resolved in 1974 were sent to this commission, but predictably the hot moment for media attention passed by the time the commission reported its findings in 1977, and inertia won the day. Could a similar failure by omission hamper privacy legislation today?

Homeland Security and Its Failures

Looking back on the years since the weak Privacy Act was adopted, controversies related to privacy have erupted with respect to banking, health care, credit, telecommunications, and other sectors. The responses followed the wave model: public attention to a problem, sharp disputes, state laws with diverging requirements, lobbyists' support for federal laws, compromises that produced weak legislation, and later administrative actions on the downside of the wave to neutralize its effect. How is the concern for privacy in the era of homeland security different from the concerns raised earlier?

First, agencies involved in protecting homeland security were often staffed as stepchildren of the police force, and the privacy issues that were the responsibility of the law enforcement sector were traditionally resolved without legislation through the Supreme Court's decisions related to rights under the Fourth and Fifth Amendments. This trend changed when law enforcement began to use telecom-

munications and financial records under divergent state laws. Lobbyists for the banking and telecommunications industries successfully urged Congress to adopt uniform specific laws to protect their companies from suits alleging abuse. Second, privacy as a concept is adaptable to particular regulatory regimes such as those that apply to banking, but homeland security is an umbrella covering dozens of programs, not all of which fit easily within the same template.

Federal protection of individuals' privacy has been an awkward guest in the basement of the rambling ranch house that is the U.S. Department of Homeland Security (DHS). When I studied the legislative proposals for the Homeland Security Act of 2002 in preparing my *Homeland Security Deskbook*,[8] I noted that they were like a child's basket of Easter candy—every piece of investigative authority that the Federal Bureau of Investigation, the National Security Agency, and the Central Intelligence Agency wanted for years was floated in Congress as a response to the embarrassment security agencies felt in the wake of the attacks of 9/11.

The issue of privacy in legislation related to homeland security was an afterthought, and the topic almost seems to have been a sop to the Democratic minority in Congress. Continuing the legislative wave analogy, the role of "chief privacy officer" was tossed into the froth at the peak of the wave. The expected bureaucratic undercutting of privacy gains began immediately: those charged with advocating for privacy concerns within the Department Homeland Security appear to carry little weight with agency personnel.

DHS' five-year record reveals a concern for privacy that is inadequate at best. So much of the department's money has been spent on local fire departments and so many ineffective bureaucracies have shared in the fiscal largesse of the billions of dollars allocated to DHS that one can easily question the merits of the government's spending policies. DHS' money has been a "green Hurricane Katrina": a torrent of taxpayer funds allotted for a legion of projects. But is the U.S. Department of Homeland Security respected in other countries? Is the U.S. immigration system streamlined? Are the country's borders secured? Have bioterrorist threats been eliminated? When one digs deeply into the topic, DHS does not come out looking very good in light of the amount of money that has been invested in its mission. This apparent failure sets the backdrop for the government's policy challenge; we must ask if all of us are so much better off in view of the loss of privacy that we have endured?

It is even easier to question the way other agencies have handled policy decisions related to privacy. Where were the privacy advocates when the National Security Agency began its intensive domestic spying? Were they at the table when the Transportation Security Administration's (TSA) no-fly lists were created? Who won the closed-door argument about target lists and secret prisons? Were the chief privacy officers included in the discussion when serious infringements of personal privacy by the FBI were condoned under the USA PATRIOT Act?

Happily, the people who have held the position of chief privacy officer at DHS have been bright and capable leaders. But where is the positive result of their efforts? A review of the Bush administration's track record on issues related to privacy reveals the lost opportunities that could have been managed so much better.

The growth of wider public opinion favoring the protection of privacy has tracked the decreasing public trust in DHS in general. Critics of federal actions can zero in on the many failings of the Department of Homeland Security: the fiasco that followed the devastation caused by Hurricane Katrina, the confusion over names on the no-fly lists, secrecy about exposure to dangerous formaldehyde levels in FEMA trailers, and the like. States are starting to push back against the REAL ID legislation in part out of concern over how DHS will protect privacy in the massive database included in the program. Where is the advocacy for privacy? Where is the sensitivity to privacy values? Where is the transparency?

DHS critics will concede that the privacy climate at the Department of Homeland Security is better than that found at the Department of Justice (DOJ), where the zealous defense of so many questionable activities—warrantless wiretapping, the concealment of tortures like waterboarding, the disdain for the FISA court's warrant requirement, the denial of Geneva Convention rights, and so forth—have put DOJ in the center of controversy, right alongside DHS. Promoting privacy inside the government is not DOJ's job; indeed, the department's Office of Information and Privacy is a zealous warrior against Freedom of Information requesters and Privacy Act challengers alike.

The point is that DHS, with a small privacy team aboard, has *not* made the convincing case that an individual's privacy really matters to the Bush administration. DHS has squandered many opportunities to explicitly justify the loss of individual privacy rights. Instead of handling the issues related to the disclosure of airline passenger lists with diplomatic sensitivity, TSA has alienated the thought leaders and public officials in Europe. When DHS defended America's privacy policies in a recent paper presented to foreign observers, I expected a somewhat apologetic or defensive tone. I was startled to find the DHS paper full of upbeat expressions defending the fact that Americans have 50 different state privacy systems and fragmented federal laws.

Predictions

In light of all these concerns, I offer 10 predictions of future developments that are likely to be the consequence of the Bush administration's attitudes toward protecting the privacy of the country's citizens:

1. Privacy issues will *not* be ignored on the 2008 presidential campaign trail. The disclosures about Barack Obama's passport in March already have shown the accuracy of this prediction.
2. Federal actions perceived as invading privacy will set off a backlash that damages the ability to gather human intelligence from informants in some ethnic communities within this country. Consider, for example, how much harm the scandal about Scooter Libby's leak to a journal-

ist caused for the CIA's program to retain and protect the identity of its covert operatives. Similarly, with respect to Islamic citizens or members of any other ethnic group, if the government disregards the group members' privacy, a channel of voluntary information flow will be cut off.

3. The United States will continue to suffer harm to its reputation by ignoring the rule of law on issues of FISA warrants, wiretapping, and Internet intrusions and deceptions. This outcome will damage our international alliances, at least until a new administration can begin a mission to repair the damage.
4. Members of Congress will be motivated to act on legislation that protects an individual's privacy in the 111th Congress, because during the 2008 campaign voters, and especially editorial boards and serious bloggers, will ask about each candidate's positions on wiretapping and secrecy in government. In my past life as a political candidate, I could attest to the truth of writer Samuel Johnson's ancient aphorism that the imminent prospect of a hanging concentrates the mind wonderfully. Facing editors of newspapers in the weeks before their re-election will assure that congressional leaders think long and hard about their position on protecting privacy rights. In the next session of Congress, remedies for actions that deprive citizens of their privacy will be expanded, and more civil litigation will follow after increasing revelations about breaches of databases and identity thefts.
5. Privacy will be seen as a more bipartisan ideal than many suspected in the past. Voters will ask tough questions about those political parties whose leaders appear to disregard privacy interests. Political parties may have serious disagreements among their factions about the issue of privacy protection, with libertarians fighting the wealthier lobbies inside the party, but whichever party one studies, privacy advocates will be seen as a potent force.
6. The claim of fighting a war and excusing all privacy deprivations will be asserted by one party. But opponents will press that party's candidates on the issue of their policy on warrantless wiretapping, data mining, and Internet snooping used to "win" the war over the next 10 or 20 years.
7. The trends to pass more legislation to protect personal privacy at the state level will frustrate the lobbyists for the business sector to such an extent that there will actually be Republicans interested in uniform federal privacy legislation that has teeth. Serious state action on privacy will induce potent lobbying for more federal privacy protection as a way to pre-empt state initiatives.
8. New federal legislation will move more toward the European Union's opt-in system, which requires individual choice before disclosure of sensitive personal data.
9. Public attention to privacy interests will continue to grow, and the media will increasingly scrutinize those who justify abandoning the privacy aspects of the rule of law in favor of expediency.
10. Finally, Congress will eventually create an independent "privacy commissioner" along the lines of the models adopted by Canada and the European Union. That individual will not lack clout and will have a real seat at the policy-making table. In March, Congress' rapid rejection of the Bush administration's budget proposal that included placing the problem-solving role for Freedom of Information Act disputes within the purview of the Department of Justice signifies that this change is coming.

The European Model

I predict that the trend between 2009 and 2016 in favor of privacy will prompt Congress to alter many of the current administration's positions on privacy protection—but only after business forces push the influence of K Street lobbyists onto Congress. Today the current is shifting toward recognition of privacy and away from the passionate secrecy of the outgoing administration. As I dare to forecast the future of the balance between privacy and security, I foresee a shift that will move the United States more toward the European model of individual privacy rights. Why should our leaders care less about privacy rights than the leaders of 27 European nations do?

Even though leaders of European Union member countries who grew up in or near Soviet-controlled regimes have a passion for privacy rights that is not shared by current U.S. leaders, it is helpful for the U.S. administration to look across the Atlantic to discern positive future trends in privacy rights that this country would be wise to adopt. The European Data Protection Directive 95/46, unlike the U.S. model, establishes a very strong presumption that the individual can prohibit government disclosure of his or her personal data. But the European directive has an exception for "public security, defense, State security … and the activities of the State in areas of criminal law." The transfer of personal private data to another nation is governed by Directive 95/46, and it requires special protective arrangements that meet the requirements for safe harbor protection. Put simply, in Europe, the government is an active guardian of individual privacy rights.

The most significant changes in adopting a more citizen-friendly, European-style trade-off include a greater attentiveness among federal agencies to the individual's right to be notified before records are used and an increase in citizens' rights to affirmatively choose whether or not to be included in records that are disclosed. The opt-in choice empowers the individual, as compared to the opt-out clause that appears in very small type that is hidden on the back of American credit card agreements.

A second significant change could be the adoption of the European Union and Canada's model of appointing data protection commissioners, or privacy commissioners, and giving them the statutory responsibility as well as the staff to assert the rights of persons claiming that their privacy has been violated. The privacy commissioner who can push back—and often does—earns the grudging respect of financial institutions as well as law enforcement agencies. Why such an independent role? I am convinced after my decades of working with privacy issues that the U.S. Justice Department cannot expect public acceptance of its bona

fides for privacy protection while the department actively litigates in favor of secrecy. An independent privacy commissioner would be a part of future U.S. privacy legislation; the current subordinate model that exists within the Department of Homeland Security is too weak and too underfunded to matter much to those executive branch officials who seem to disdain individual privacy protections.

Over the past several years, collisions between privacy and security have become frequently reported stories in the news media. Member nations of the European Union that have fought against terrorism for years—such as Great Britain, France, and Spain—have accepted the policy trade-offs that come with the need to identify airline passengers. The whole world watched as the Department of Homeland Security bungled the diplomatic confrontation over screening airline passenger manifests and then blustered to force Europe to meet TSA's demands. TSA is already among our most ridiculed bureaucracies; its handling of privacy will undoubtedly improve under the new administration as the agency's managers are replaced.

Avoiding the "Surveillance Society"

Peter Schaar, Germany's data protection commissioner, has warned that a "surveillance society" could be the result of the overcollection of personal communications and other private data. He noted that, when fighting terrorism, he and his peer group of data protection officers have no objection to the collection and exchange of personal data among law enforcement authorities. But proportionality is lost when the personal information about 5,000 individuals is gathered in order to find five suspects. Moreover, according to Schaar, it would be wrong for governments to use security as a rationale for collecting masses of data "without any initial suspicion and concrete danger." He has urged that data releases be strictly limited to their law enforcement purposes and that "the rights of innocent citizens must be guaranteed" by implementing stronger data protection regulations. Commissioner Schaar called for greater authority to be vested in independent data protection authorities to allow them to conduct cross-border data protection audits. Schaar's signal to the United States should be heeded as Congress considers the next wave of privacy legislation.

What happens when the perceptions about the importance of privacy vary so greatly between Main Street and Pennsylvania Avenue in Washington? Consider the analogous lessons from "human factors" experts with respect to consumer warnings: people freely accept a risk with a product when they can choose a benefit for themselves, but they are outraged when a risk is imposed on them without their willing consent. Similarly, we accept significant risks when we ski or drive sports cars, but we oppose the more remote risks of explosions that a large nearby factory may impose because the risk occurs without their neighbors' choice or consent. Human factors experts call this category of risks to which the pubic has not consented the "outrage" factor. Put simply, when a party imposes or commands an action that the public expects to be an individual choice, the public pushes back.

In the private sector, the value of individual privacy can be exchanged for things the public wants. Individuals can go on Facebook™, for example, and meet new friends in exchange for personal disclosures. If we want to have free e-mail, we can choose to give Google™ some personal data and receive tailored advertising messages. These conscious trade-offs of privacy interests represented well-considered choices, and the privacy deprivations are voluntary.

We could choose to give up privacy if we were convinced the surrender of rights assured security benefits, but the benefits of DHS activities are poorly communicated or never communicated. The outrage that citizens feel about having risks imposed on them by a factory, therefore, is analogous to the outrage citizens feel when federal spying is imposed and overrides personal privacy rights.

Conclusion

The prospects for legislation will be different when debate over the Privacy Act is reopened in 2009–2011 under the next presidential administration. Because privacy has become a pocketbook issue for voters, more members of Congress will pay attention to the issue. Moreover, privacy is an international trade issue; therefore, lobbyists will push legislation that makes the U.S. system more compatible with that of the European Union and those of other nations. Historians will look back at the years 2001–2008 as a period of great distrust of the statements and omissions by the administration, and that distrust will empower a new wave of public support for protecting the individual's right to privacy.

Surf's up. Catch the wave of public perceptions about privacy, which is so important to the rule of law. The alternative is to sit on the beach, keep your head in the sand, and leave the privacy debate to others. Please consider these views as you struggle each day with your piece of the puzzle of the balance between privacy and security in modern America. **TFL**

Professor Jim O'Reilly of the University of Cincinnati College of Law has authored 35 texts and lectured internationally on privacy. He formerly chaired the FOIA/Privacy committee of the FBA Administrative Law Section. He is a former police officer and now is vice-mayor of an Ohio city.

Endnotes

[1]Samuel Warren and Louis Brandeis, *The Right of Privacy*, 4 Harvard L. Rev. 193 (1890).

[2]*Griswold v Connecticut*, 381 U.S. 479 (1965); *Roe v Wade*, 410 U.S. 113 (1973).

[3]5 U.S.C. 552a.

[4]The history is recounted in James O'Reilly, Federal Information Disclosure, vol. 2, chap. 20 (3d ed., 2007 Supp.)

[5]James O'Reilly, Federal Information Disclosure (3d. ed., 2008 Supp.).

[6]*Id.*, vol. 1, sec. 3:9.

[7]5 U.S.C. 552a(a)(5), (b).

[8]James O'Reilly, Homeland Security Deskbook (2007 Supp.).