ENFORCING PRIVACY

Building American Institutions to Protect Privacy in the Face of New Technology and Government Powers

NOVEMBER 2009

www.aclu.org

ENFORCING PRIVACY:
Building American Institutions to Protect Privacy in the Face of New Technology and Government Powers

November 2009

Written by Jay Stanley

THE AMERICAN CIVIL LIBERTIES UNION is the nation's premier guardian of liberty, working daily in courts, legislatures, and communities to defend and preserve the individual rights and freedoms guaranteed by the Constitution and the laws of the United States.

National Office
125 Broad Street, 18th Floor
New York, NY 10004
212-549-2500
www.aclu.org

EXECUTIVE SUMMARY

Privacy laws are of limited value if institutions for enforcing such laws do not exist. The United States, unlike nearly every other advanced-industrial nation, does not have an independent data protection official or privacy commissioner to fill that role. We recommend that Congress take several steps to bridge this gap:

1. Activate the independent Privacy and Civil Liberties Oversight Board (PCLOB) and expand its scope and powers to turn it into a full-fledged privacy body with oversight of all government agencies.

2. Supplement the strengthened PCLOB with multiple overlapping layers of privacy protection, by creating a statutorily mandated Privacy Advisor within the White House's OMB, and bolstering and expanding federal agency privacy offices.

3. Create an independent federal privacy commission to serve as a full-fledged private-sector privacy regulator.

1. THE NEED FOR U.S. INSTITUTIONS TO ENFORCE PRIVACY

The United States urgently needs stronger privacy oversight institutions to serve as a countervailing force as the computer and telecommunications revolutions change the privacy landscape for Americans and create new opportunities for large institutions to grab more power at the expense of ordinary people. Only by creating such institutions can we ensure that American values are preserved and the rights and interests of ordinary people are protected.

The fact is, the rules of the game are changing. Advances in technology, with all the conveniences and benefits they bring, also open up new ways of tracking, sorting, labeling and controlling people. We are increasingly living in a world where our every word, movement and transaction is captured and subject to scrutiny and judgment. Americans' lives are increasingly controlled by their data – or to be more precise, data about them that is controlled by others.

But, just because something *can* be done does not mean it should be; many of the new techniques that the government and private companies are rushing to deploy are not consistent with our values and our freedom. Privacy rights are one of the crucial underpinnings of our democratic society, yet in the United States, as big institutions rush to exploit the latest computer technology, privacy interests are not sufficiently represented at the table if they are present at all.

The private sector has become extremely aggressive in gathering data about consumers. And Americans share information with the federal government (or someone else shares their information for them) in a dizzying breadth of areas – wage and employment data held by the Social Security Administration, medical information held by Medicare or the Veteran's Administration, financial data held by IRS, educational records held by the Department of Education, and much more.

A gigantic security establishment, with miniscule oversight

The nation's rapidly expanding security establishment, in particular, is exploring the uses of such information to track, sort and control individuals. The National Security Agency employs approximately 30,000 people. The CIA employs another 20,000. The U.S. government intelligence establishment as a whole, with a 2008 budget of at least $57 billion, must employ far more.[1] Yet the independent oversight structures that have been created to oversee these vast, city-sized

institutions are pitifully small and weak: a few members of Congress and their staff (many of whom, once they are informed of classified activities, view themselves as compromised in their ability to take action based on that knowledge); inspectors general who report to the heads of the agencies they oversee; and a frequently deferential press establishment that is faced with aggressive assertions of secrecy and all too often dependent upon the rare individual whistleblower willing to risk his or her career to bring abuses to light.

It's not as if there is no record of abuse of surveillance power. During the Cold War and Civil Rights eras, the CIA and FBI engaged in criminal behavior that represented a direct assault on individuals' rights, the rule of law, and the Constitution. More abuses were committed during the Bush Administration. More broadly, the historical record clearly shows that where secrecy and lack of accountability exist, abuse of power – not to mention incompetence and waste on a stunning scale – is inevitable.

The United States lags behind other nations

Other nations around the world have created privacy and data protection commissioners with responsibility for protecting their citizens, and the powers to carry it out. Every other advanced-industrial nation other than the United States, Japan and South Korea has some form of such an office [see box]. In many cases, these officials have considerable powers – not only to respond to complaints, but to proactively patrol against problems, subpoena information, and require action in response to problems. The Italian privacy authority, for example, has broad powers to inspect the files of government agencies – including intelligence agencies – order remedial actions, impose fines, or directly prosecute violations of the law.[2]

WHO'S GOT A PRIVACY COMMISSIONER?

among the high-income democratic[3] nations:

Australia	☑
Austria	☑
Belgium	☑
Canada	☑
Czech Republic	☑
Denmark	☑
Finland	☑
France	☑
Germany	☑
Greece	☑
Hungary	☑
Iceland	☑
Ireland	☑
Italy	☑
Japan	☐
Korea	☐
Luxembourg	☑
Netherlands	☑
New Zealand	☑
Norway	☑
Portugal	☑
Slovak Republic	☑
Spain	☑
Sweden	☑
Switzerland	☑
United Kingdom	☑
United States	☐

The European Union's Data Protection Directive requires member states to have "supervisory authorities" monitoring privacy that have "*complete independence* in exercising the functions entrusted to them." The directive also requires member states to give supervisory authorities the power to conduct investigations, gain access to information relevant to those investigations, hear complaints, issue reports, initiate legal proceedings, and intervene. Governments are also required to consult the commissions when drafting relevant regulations.[4]

Stronger and more independent privacy oversight institutions would also be consistent with our nation's international human rights treaty obligations – especially concerning the right to privacy enshrined by article 17 of the International Covenant on Civil and Political Rights, ratified by the United States in 1992.[5]

The United States needs a better privacy-oversight institutional framework. It will look different from other countries because, unlike nations with parliamentary systems of government, the United States operates under distinct legislative and executive branches under the principle of separation of powers. How to create uniquely American structural checks and balances to protect privacy and other civil liberties is the question that this report seeks to answer.

Privacy laws need strong institutions to back them up

Even strong privacy laws need institutions to enforce them and defend them, or they may wither on the vine (and in our jurisprudence). As privacy scholar David H. Flaherty wrote, "[I]t is not enough simply to pass a data protection law in order to control surveillance; an agency charged with implementation is essential to make the law work in practice."[6] Statute and enforcement mechanism are two sides of the same coin; a law that is not enforced is like no law at all – especially a law governing something such as privacy, where the pressures to violate privacy are, in the course of human affairs, constant, universal, and unremitting.

The courts, of course, are available for redress. But many technologies today are so novel, and the pace of development so rapid, that our legal system simply has not kept up. Unfortunately, our judiciary is sometimes slow to adapt the Constitution to the realities of new technology. It took almost 40 years for the U.S. Supreme Court to recognize that the Constitution applies to the wiretapping of telephone conversations.[7]

Over three decades ago, Congress enacted a landmark piece of government reform legislation known as the Privacy Act of 1974. This statute, the closest thing the United States has to an overarching privacy law, sought to create

a range of rights and protections in order to "promote accountability" with respect to the "personal information systems and data banks of the Federal Government."[8]

Unfortunately, the act is riddled with loopholes and exceptions that have grown over time. Some agencies, especially law enforcement, have taken to exploiting the act's exemptions to avoid compliance with basic privacy policies. Many of the Privacy Act's protections have eroded, in part, because there has been no counterbalancing institution to push back and defend it when agencies seek to interpret away its often inconvenient provisions.

A variety of other laws govern privacy among government agencies and across the private sector. These laws make up a patchwork of inconsistent, often tangled and complicated, yet simultaneously weak and incomplete rules. This inconsistent situation – video rental records are more strongly protected than Americans' banking or health data, for example – must be addressed by Congress through the enactment of an overarching privacy law that will put clear, fair privacy standards into law (without endless loopholes) and create stable expectations for businesses, government and individuals alike.

Whether the United States eventually enacts a meaningful version of the Fair Information Practices that the rest of the industrialized world has embraced,[9] or continues to limp along with an ever-more-complicated patchwork of laws, the need is urgent for a vigorous privacy oversight institution in the United States.

Critical Functions

With government agencies rapidly assuming new powers, and technology opening up new avenues for surveillance on what seems to be a weekly basis, what functions should privacy institutions fill? Even if not all carried out by the same body, crucial functions include:

- **Pro-active auditing and oversight.** A privacy office should not sit around waiting for reports of problems to reach it, but should engage in pro-active oversight activities to prevent, detect, and ferret out trouble.

- **Investigation.** When problems or scandals do arise, a privacy office should conduct a proper investigation and determine what happened and why, and how the problem could be prevented. For example, when the public learned that the Bush Administration NSA engaged in illegal

domestic wiretapping with approval at the very top of the executive branch, Americans needed officials in a position to launch an independent investigation on behalf of the public, and the power to do so effectively. Unfortunately, no such position existed.

- **Public disclosure.** A privacy office should not just investigate and monitor the behavior of government agencies, but in a democracy should disclose its findings and recommendations (and generally distribute information) to the Congress, the executive branch, and the public.

- **Pro-active policy leadership.** With the privacy and technology landscape constantly in a state of rapid change, a privacy officer is needed not just to perform specific bureaucratic functions but also to provide broad public leadership and guidance on how to protect privacy and other liberties.

- **Counsel, review and consultation.** When security agencies or other government bodies are considering new policies and programs, it is good to have privacy interests and expertise at the table on the inside – people who can vet such ideas at the earliest stages, steer officials away from bad ideas, and generally serve as an institutional representation for the values of privacy in the policy process.

- **Complaint resolution.** A privacy office should be responsive to specific complaints from individuals and institutions.

Crucial Powers & Attributes

In order to carry out these functions, any privacy-protecting institution must possess several key characteristics, regardless of its organizational structure and whether it oversees government or the private sector:

- **Independence.** Independence from potential subjects of investigation is crucial. No one can provide oversight over a person or institution that holds power over the supposed overseer. The actual and perceived effectiveness of a watchdog depends upon complete independence.

- **Access to information.** Without the ability to compel the production of information, no entity will be effective at providing oversight in the face of bureaucracies in law enforcement, intelligence, homeland security, and national security. Those bureaucracies have shown a repeated willingness

over the years to use their secrecy powers not to protect national security but to cover up incompetence and illegality and other embarrassments and generally thwart oversight.[10]

- **The power to order compliance.** A true enforcement body should have the power to enforce compliance with the law, subject to judicial review, as opposed to merely making a public report or falling back upon the courts.

- **A broad mandate.** An oversight body should be empowered to provide leadership on privacy issues by a provision authorizing the body to comment upon legislative provisions, government or private-sector plans for new programs or services, new technologies, or other developments that have privacy implications, and to conduct research on current and emerging trends in such areas.

- **Sufficient resources.** A broad mandate and strong legal powers do no good if an agency lacks the staff and resources necessary to make use of them. Some privacy officials complained that they simply didn't have sufficient resources to do anything but react to complaints, not to mention carrying out the full extent of their powers under the law.

2. A MULTI-LAYERED APPROACH TO PRIVACY OVERSIGHT

The overlapping and sometimes contradictory functions needed to protect our privacy properly cannot all be performed by a single institution. Instead, we recommend a multi-layered approach to the institutional protection of privacy in the United States – an approach that includes both privacy officials working within government agencies, and a truly independent, outside oversight body.

Privacy oversight in the American system

The United States needs a major new privacy oversight institution – the American equivalent of our allies' independent Data and Privacy Commissioners. We cannot simply copy our allies but must create a uniquely American institution, since we do not operate under a parliamentary system. In Canada, for example, privacy officials' independence is made possible by the fact that the commissioner reports directly to Parliament generally rather than to a minister in the government formed by the majority party. In the United States, however, our system of separation of powers (in which the executive branch is separate from the legislative) means that the creation of independent oversight institutions must be approached differently.

Options for structuring privacy oversight in the U.S. might include:

- **A privacy officer within the executive branch.** Such a position, being directly or indirectly under the president, would lack independence. Indeed, several years ago the International Conference of Data Protection and Privacy Commissioners refused to recognize the Chief Privacy Officer of the U.S. Department of Homeland Security precisely because it judged the position to be insufficiently independent to qualify for membership. A privacy officer within the executive branch might help the president make better policy, but such an office would not be well-suited for challenging or investigating executive branch officials.

- **An arm of Congress.** The model would be the Government Accountability Office (GAO). However, the office would raise separation-of-powers problems. The GAO is an arm of Congress, but its chief, the Comptroller General of the United States, is appointed by the President (under a process that involves recommendations from the leadership of Congress) for a single, non-renewable term of 15 years. In the wake of *Walker v. Cheney* (a lawsuit filed against the Bush Administration by the GAO over

the records of an energy task force led by Vice President Dick Cheney, which the GAO lost and did not appeal), the GAO's ability to access executive branch information as part of its investigations is limited.[11] On the other hand, while insufficient on its own, the GAO has produced good work on privacy issues and can be counted upon to remain a key part of the overall oversight landscape.

- **An arm of the judiciary.** The judiciary's independence is without question. However, under the Anglo-American legal system the judiciary does not conduct investigations or pro-active oversight. It is purely reactive in that it only decides cases that are brought before it.

- **An independent federal regulatory commission.** Among the most prominent of the many such institutions are the Federal Trade Commission (FTC), the Federal Communications Commission (FCC) and the Federal Election Commission (FEC). The independent federal commission is the best model for an institution designed to protect privacy within the U.S. system of government.

The independent commission model

Independent regulatory agencies have long been used by Congress as a way to insulate agencies within the executive branch from political pressures. Congress has relied upon this strategy for many years, going back to the creation of the Interstate Commerce Commission (ICC) in 1887. Since then Congress has created numerous independent commissions, including such bodies as the FTC, the FCC, the FEC, the Commodity Futures Trading Commission, the National Transportation Safety Board, the U.S. International Trade Commission, and others.

These institutions typically consist of five or six members appointed by the President and confirmed by the Senate for staggered terms of five to nine years, with no more than three members permitted to be from the same political party. The president generally does not have the power to remove commissioners (the Supreme Court struck down an attempt by Franklin Roosevelt to fire a member of the FTC in 1935).[12] The powers of such commissions typically involve investigating complaints and seeking voluntary compliance or filing administrative or legal complaints where wrongdoing is found; and rulemaking power that allows them to issue regulations to carry out the goals that Congress has authorized them to pursue.

3. RECOMMENDATIONS

We recommend three primary steps to bring U.S. privacy oversight up to a sufficient international standard:

1. Create an independent commission to cover privacy in the government by expanding the mission of the Privacy and Civil Liberties Oversight Board (PCLOB).

2. Supplement a strengthened PCLOB with multiple overlapping layers of privacy protection.

3. Create an independent commission to serve as private-sector privacy watchdog.

RECOMMENDATION #1:
Create an independent commission to cover privacy in the government by expanding the mission of the Privacy and Civil Liberties Oversight Board

It is always easier to build upon existing institutions than it is to create new ones from whole cloth. An institution already exists on the books that is well-positioned to take on the full role of providing privacy oversight, at least with regards to the security establishment within our own government, and provided that Congress repairs several shortcomings with regard to its powers. That institution is the Privacy and Civil Liberties Oversight Board.

The PCLOB was created by Congress in 2004 on the recommendation of the 9/11 Commission.[13] However, as initially structured it was a meaningless shell without any teeth whatsoever. It was created under and supervised by the Executive Office of the President and consisted of 5 members hand-picked by the White House. The only Democrat placed on the board by President Bush quickly resigned when the White House ordered over 200 deletions and other revisions to the board's first, unanimously approved report.[14]

In 2007, however, a new Congress removed the PCLOB from the White House and made it an independent agency with the mandate to monitor the impact of U.S. government actions on civil liberties and privacy interest. In the legislation Congress found that while the government may need new or augmented powers

to fight terrorism,

> This shift of power and authority to the Government calls for an enhanced system of checks and balances to protect the precious liberties that are vital to our way of life and to ensure that the Government uses its powers for the purposes for which the powers were given.[15]

Unfortunately, President Bush refused to nominate one of the candidates put forth by leaders in Congress, who traditionally select the commissioners from the opposite party from the president. In retaliation the Senate refused to confirm any of Bush's GOP nominees. Because the terms of the original board members expired in January 2008, the revised board was never brought into existence during President Bush's term.[16]

Once the board is actually filled and staffed, even in the absence of the adoption of proposals offered herein, the PCLOB will possess some significant powers.

The new, independent Privacy and Civil Liberties Oversight Board
Like many independent federal commissions, the reconstituted PCLOB consists of a chairman and four additional members appointed by the President and confirmed by the Senate. They serve for overlapping six-year terms with no more than three members being from the same party.

The board's mandate is to "analyze and review actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties" and to "ensure that liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism."[17]

That is a tall order for a small and still-obscure board with a congressionally authorized fiscal 2009 budget of less than $7 million, facing an intelligence establishment with a budget of at least $57 billion, and a security establishment overall that is far larger still.[18]

To accomplish this daunting task, Congress gave the PCLOB powers to:

- Issue reports to Congress and, to the greatest extent possible, to the public.

- "Have access . . . to all relevant records ... including classified records" necessary to carry out its responsibilities.

- "Interview, take statements from, or take public testimony from personnel" of any element of the executive branch.

- "Request information or assistance from any State, tribal, or local government."

- When supported by a majority of the board, ask the Attorney General to issue a subpoena on behalf of the board. Within 30 days of a board request, the AG must either comply or provide a written explanation for a denial to the board and to the House and Senate Judiciary Committees.[19]

Crucial Powers & Attributes	Status
Independence	The PCLOB's status as an independent agency ensures that it will be independent as far as possible within the U.S. system of separation of powers.
Access to information	Congress endowed the PCLOB with significant powers to obtain information "necessary to carry out its responsibilities" and to issue subpoenas through the Attorney General. However, PCLOB should have its own subpoena power, and its mission needs to be expanded to cover all government agencies, not just those related to anti-terrorist efforts.
The power to order compliance	Congress should explore how the PCLOB can be given authority to act when confronted with violations of privacy and civil liberties.
A broad mandate	The PCLOB's congressional charter is quite broad, encompassing many of the crucial oversight functions needed in a privacy oversight body such as conducting oversight over executive branch policies and actions, ensuring consideration of privacy in policy formation, and informing the public. However, it should be expanded in scope to all of government (rather than just anti-terrorism programs), given additional powers to overcome secrecy and access information by subpoena.
Sufficient resources	Congress must give PCLOB resources commensurate with its needed role serving as a check on the gigantic U.S. national security establishment. A few million dollars and a staff of ten will amount to little more than a gesture toward the establishment of a meaningful oversight body.

What is still missing from the Oversight Board

The PCLOB as reconstituted in 2007 is a good start toward an institution capable of performing genuine oversight over the U.S. security establishment. Of the key powers and roles listed above, it includes independence, fairly strong powers to access information in investigations, and a mandate that allows it to resolve complaints, engage in pro-active oversight as well as counsel, review and consultation, carry out investigations, and provide pro-active policy leadership.

Even putting aside its exclusive focus on the government (as opposed to private sector), the PCLOB still falls short of a true privacy commission. The problems that remain include:

- **It is too narrow in scope.** Even as a government-focused entity, the oversight powers given to the PCLOB are too specific. They are all restricted to "elements of the executive branch relating to efforts to protect the Nation from terrorism." However, privacy threats emanate from across the executive branch, and a privacy agency must be able to respond to any of them. Even within the national security state, terrorism has become the primary justification for increased surveillance and other powers across the U.S. government, but it is not the only one. Before terrorism, the threat justifying expansion of the U.S. security establishment was communism. Domestic crime, drug trafficking, illegal immigration, the abuse of public benefits – even such problems as "deadbeat dads" – have at various times been used to justify the expansion of government powers and the diminution of personal privacy standards. By restricting the PCLOB to terrorism-justified invasions of privacy, Congress has left large openings for mischief and the possibility that as times change it will render the Board largely irrelevant. Oddly, if the PCLOB takes up its mission even without further reform, Americans would have privacy protections in the national security arena, but much less protection in areas where the national interest in breaching personal privacy is much less compelling. The PCLOB should be turned into a commission charged with overseeing the entire federal government.

- **Over-classification.** The chronic problem of excessive secrecy within our government will pose an ongoing threat to the effectiveness of the PCLOB. Hamstrung by secrecy rules, Members of Congress informed about the Bush Administration's domestic NSA spying program were unable to provide any kind of counterbalance to executive abuses of power.[20] In certain situations, such as the uncovering of a brazen, shameless violation of the law, the board must have the power to share its findings or it will be

useless. Congress must give the PCLOB a meaningful power to challenge agencies' classification powers when they are abusing those powers to cover up wrongdoing or incompetence or to prevent legitimate public debate. Checks and balances must be extended to the power of secrecy or secrecy will prevail every time. Implementation of such a power could be achieved through appeal to the Information Security Oversight Office (ISOO) at the National Archives and Records Administration (NARA), for example, together with a requirement of expedited judicial review. Alternatively, Congress could grant the board the independent power to declassify information when it concludes that an agency has abused its classification authority.

- **Enforcement.** The PCLOB has no power (other than going to court) to order any government agency to change its practices or otherwise enforce the law. When in April 2008 the outgoing Italian government decided to publish the income tax returns of all Italian citizens on the Internet, the Italian data protection authority did not just condemn the action, or hold hearings, or file a court case. The authority *ordered* the information taken down, and it was. Congress should explore how the PCLOB can be given commensurate authority to act when confronted with a flagrant violation of the law.[21]

- **Resources.** The PCLOB currently exists only on paper. Once it takes shape through the appointment of members and hiring of staff, Congress must increase its budget and staff to a level commensurate with the board's task of overseeing the $57 billion intelligence establishment and other security agencies like Homeland Security, the FBI, and the non-intelligence parts of the Defense Department. A handful of staffers on a shoestring budget will not be enough.

- **Subpoena power.** Congress gave the PCLOB the power to ask the Attorney General to issue subpoenas on its behalf, and the Attorney General the power to deny the request. This unnecessary curb on the PCLOB's independence should be remedied by giving the board its own subpoena power.

- **Coordinating role.** Congress gave the PCLOB a good start toward playing the role of one privacy watchdog among several: it charged the board with receiving and reviewing "reports and other information from privacy officers and civil liberties officers" in other agencies, with making recommendations to such privacy officers, and where

> appropriate, coordinating "the activities of such officers on relevant interagency matters."[22] As the PCLOB's authority is expanded beyond the scope of anti-terrorism initiatives, its coordinating role should likewise be expanded to encompass the whole range of privacy issues within government. Ultimately, PCLOB should be positioned to create and maintain a broader government privacy oversight community, including agencies, inspector generals' offices, OMB, and the PCLOB itself. Congress should seek to increase the likelihood that even privacy officials who report to privacy-hostile political leaders will be guided and restrained by professional, personal, and reputational ties to such a community.

One function that privacy commisioners in many countries have is to be responsive to individual complaints. In many European nations and Canada, officials have a duty to respond to complaints from individuals and others within a certain period of time. This system guarantees that problems will be addressed, and that individuals will receive attention for their complaints. However, data-protection authorities in some countries have found that complaint resolution can absorb all an agency's time and resources – especially if there are insufficient funds for activities other than complaint resolution. Congress should establish a separate division of the PCLOB with its own budget to respond to individual complaints. Failing that, Congress should charge PCLOB with generally monitoring and analyzing individual complaints to identify patterns and problems but not necessarily to respond individually to each one.

Given the strong start that the PCLOB represents, its conformance to the optimal independent commission model, and the difficulty of creating a new institution from scratch, it makes the most sense to expand and augment the powers of the PCLOB, while retaining the characteristics that give the PCLOB strength and independence (especially its structure as an independent commission with overlapping 6-year, Senate-confirmed commissioners).

Critical Functions	How they will be carried out
Pro-active auditing and oversight	The PCLOB has been charged by Congress with performing an oversight function, continuously reviewing the implementation of executive branch policies and rules. It is also tasked with overseeing agency privacy offices. However, the PCLOB needs additional powers to fulfill that role properly. Agency privacy officials and the OMB Privacy Advisor would also play an important oversight role, having less independence but greater access to executive decisions makers.
Investigation	The PCLOB has been chartered to "investigate and review" government actions to ensure that privacy and civil liberties are being adequately considered. However, the PCLOB's powers need to be expanded for it to fully perform this role – and sufficient staff and resources are vital.
Public Disclosure	PCLOB is charged with testifying before and delivering reports to Congress and the president "in unclassified form to the greatest extent possible," and making its reports "available to the public to the greatest extent that is consistent with the protection of classified information."
Pro-active policy leadership	Not explicitly discussed in the statute creating the PCLOB, but given the PCLOB's independence, such leadership would be likely to emerge, varying with the vigor and energy of the chair and other members.
Counsel, review and consultation	The PCLOB has been chartered with providing "advice and counsel on policy development and implementation" to the executive branch. Agency privacy officials and the OMB Privacy Advisor would also play this role.

RECOMMENDATION #2:
Supplement the strengthened PCLOB with multiple overlapping layers of privacy protection

We recommend that Congress set up a two-part system for privacy oversight of government. The foundation must be the PCLOB-based independent regulatory commission discussed above. But non-independent privacy offices within the executive branch can also play an important role in a system of multiple, overlapping layers of privacy protection. Toward that end, we also recommend a White House privacy counselor and a significant expansion of the mandate of the agency privacy offices.

A statutory White House position of privacy counselor
Congress should create a statutorily mandated privacy position within the White House's Office of Management and Budget, with an explicit mandate to cover public and private sector privacy concerns.

In 1999, President Clinton named Peter Swire as the first U.S. Chief Counselor for Privacy. In that position, Swire reports that he was able to have a significant behind-the-scenes influence on the policy-making process. Much of that influence came through the process of "clearance." As policies were run by him in the process of internal consideration, he could point out problems and, where necessary, elevate policy decisions to higher-level authorities. With that simple power, as Swire sums it up: "you can block a lot of dumb proposals."[23]

On the other hand, as a political and policy-making insider, Swire was poorly positioned to serve as an ombudsman or enforcement official, because his ability to vet proposed policies required that he be trusted by those floating policy ideas. Such trust would not last if he protested in public about administration shortcomings in policy or implementation. While some internal White House advocates in other areas spoke freely in public and were then shut out of internal deliberative processes, Swire reports, "I kept message discipline. I made arguments on the *inside*; to be effective it was most important for me to my keep internal credibility intact."[24]

There is a tradeoff between the need for independence among oversight officials – the ability to be frankly and publicly critical without bias toward the interests of the President or administration – and the useful role that privacy officials can play on the inside. In addition to – but most definitely NOT instead of – creating an effective independent privacy oversight body, Congress should establish a

permanent privacy-related official at OMB.

OMB currently has more power over existing government practices than any other agency. The Privacy Act of 1974 gave OMB authority to issue guidelines and regulations[25] and OMB has powers under other statutes such as the E-government Act and the Paperwork Reduction Act.[26] However, OMB has never issued formal regulations under the Privacy Act. OMB rarely issues formal regulations, but the agency has never shown much interest in its privacy role. Except for the period when the original Privacy Act guidelines were written in 1975 and when Peter Swire was the privacy counselor between 1999 and 2001, privacy staffing at the Office of Information and Regulatory Affairs at OMB was typically less than one full-time person.[27]

Bolster and expand agency privacy offices

In much the same way as a White House privacy chief, a privacy office within each federal agency can serve an important function. Existing agency privacy officials should be retained and their powers expanded consistent with their roles as inside-agency watchdogs.

In 1998, President Clinton issued a memorandum requiring all agencies to designate a senior official within each agency to "assume primary responsibility for privacy policy."[28] Under this order, echoed in a similar 2005 memorandum from OMB[29], any official could be designated – including one with other heavy responsibilities such as an agency's Chief Information Officer. As a result, privacy was often an afterthought for those ostensibly in charge of it.

The nation's first statutorily mandated privacy officer was created in the Homeland Security Act of 2002, which designated a Chief Privacy Officer for the new Department of Homeland Security. The law gave that official the explicit duty to ensure compliance with Fair Information Practices. The officer was also charged with ensuring that "the use of technologies" does not erode privacy, evaluating legislative and regulatory proposals, conducting privacy impact statements, and reporting to Congress. The officer reports directly to the DHS secretary.[30]

In 2007, Congress increased the number of statutory privacy officers to eight, adding the Departments of Defense, Health and Human Services, Justice, State, Treasury, the CIA, and the Office of the Director of National Intelligence.[31]

Notwithstanding these actions, further steps are needed. Congress should:

- **Expand the privacy officer requirement to all other agencies.** Congress gave the PCLOB the power to require a chief privacy officer in any other "department, agency, or element" of the executive branch, so once PCLOB's mandate is expanded beyond the "war on terror" it could also accomplish this end.[32]

- **Increase the power and visibility of agency privacy offices.** Although privacy officers reporting to agency heads will never be as independent as a commission, they can certainly be given tools to increase their internal clout and effectiveness. Congress should bestow such offices with subpoena power, broader power to initiate investigations, the power to report directly to Congress, and appointment to fixed terms.[33] Along with instruments such as Privacy Impact Assessments, such powers are steps that can help ensure that agency privacy offices are systematically included in internal policy deliberations and other processes. [34]

RECOMMENDATION #3:
Create an independent commission to serve as private-sector privacy watchdog

Even granted all the powers we recommend, the reformed PCLOB would not address the growing private-sector threat to privacy. Nor does it necessarily makes sense to try to expand the PCLOB so far beyond its current mission. The American people need an institution with sufficient power to serve as a genuine privacy watchdog in the private-sector arena.

One option for creating such an institution would be to create a new institution, a Federal Privacy Commission. The other option would be to expand the charter of the existing independent commission that has the most involvement in consumer privacy issues, the Federal Trade Commission.

Proponents of a new commission say that historically, the FTC has been too focused on other missions to show promise as a genuine privacy commission. They say that the risk is too great that privacy would become an unwanted stepchild at the commission. In addition, most of the FTC's authority comes from Section 5 of the Federal Trade Commission Act of 1914, which charges the commission with preventing "unfair trade." As a result of that language, the commission's charter has allowed the FTC to address privacy issues, but ensured that it has been narrow in the way those issues are approached. The

FTC has no authority to judge or impose the Fair Information Practices or any other substantive privacy standards in the private sector. Rather, it cracks down on companies that *promise* to conform to a certain standard of privacy – and then fail to do so, a breach of promise that brings them under the commission's "fair trade" authority. Currently, companies that conduct themselves in the most abominable manner with regard to privacy – but never make any claim or promise to the contrary – cannot be touched by the FTC.

On the other hand, the advantage of expanding the FTC would be that, rather than creating a new institution from scratch, Congress could simply expand the charter of an existing commission to bestow it with the functionality of a full-fledged privacy commission. Its existing expertise on privacy, combined with a new charter and the resources to fulfill that mission, could change its existing orientation, and the FTC could evolve into a very effective privacy oversight body. The FTC has already been involved with enforcing privacy rights and its budget and staff expertise would likely dwarf that of any brand new agency. Moreover, Congress has already granted the commission authority to oversee privacy through a variety of acts, including the Financial Services Modernization Act, the Fair Credit Reporting Act and the CAN SPAM Act. The FTC would likely oppose efforts to take away its privacy authority and hand it to a new body.

On balance, it makes more sense for Congress to expand the FTC. It should charge the commission with enforcing the full Fair Information Practices (and not a weaker version) in the commercial sector.[35] The United States is one of the only advanced-industrial nations in the world that has not enshrined these core concepts, which are generally regarded around the world as tantamount to human rights principles, as rights for its citizens.

As part of the FTC's new role, Congress should direct the commission and the PCLOB to coordinate on matters where public and private sector privacy issues overlap, and ask for a joint report with recommendations. Public-private overlap is a growing problem as we witness the emergence of what the ACLU has called a "Surveillance-Industrial Complex" in the United States, in which the government increasingly leverages and commandeers the information tracking and collection abilities of the private sector for its own ends.[36] And the private sector collects even more personal information to supply to its government customers.

CONCLUSION

The United States has an enormous security establishment with strong secrecy and other powers, without sufficient institutional checks and balances to counterbalance all that power. One way to remedy such a gap is to institutionalize privacy protection in the way that nearly all other economically advanced democracies have done.

Congress should start by expanding the scope and powers of the already created independent Privacy and Civil Liberties Oversight Board to turn it into a full-fledged privacy body with oversight of all government agencies. The strengthened PCLOB should be supplemented by multiple overlapping layers of privacy protection. The creation of a statutorily mandated Privacy Advisor within the White House's OMB and the bolstering and expansion of federal agency privacy offices will accomplish that end.

Finally, Congress should expand the mission of the Federal Trade Commission to include the duties and powers of a full-fledged private-sector privacy regulator charged with enforcing the Fair Information Practices recognized around the world as the embodiment of human beings' right to privacy.

ENDNOTES

1 CIA employee numbers are classified. One site that reports a figure is http://www.soyouwanna.com/site/syws/cia/ciafull.html. On NSA see National Security Agency, "About NSA," available online at http://www.nsa.gov/about/about00018.cfm#7; the DNI reported a 2008 budget appropriation of $47.5 billion, but Steven Aftergood of the Federation of American Scientists pointed out that this estimate omits the Military Intelligence Program. Steven Aftergood, "Intel Budget Disclosure and the Myths of Secrecy," Secrecy News, Oct. 28, 2008; online at http://www.fas.org/blog/secrecy/2008/10/budget_disclosure.html; Office of the Director of National Intelligence, "DNA Releases Budget Figure for 2008 National Intelligence Program," press release, Oct. 28, 2008; online at http://www.dni.gov/press_releases/20081028_release.pdf.

2 Italian Data Protection Code (2003), http://www.garanteprivacy.it/garante/document?ID=727068, esp. Sections 154-172. For other examples see the German Bundesdatenschutzgesetz (Federal Data Protection Act) (1977), last amended in 2006, http://www.bfdi.bund.de/nn_535764/EN/DataProtectionActs/DataProtectionActs__node.html, or France's Act No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (1978), http://www.cnil.fr/fileadmin/documents/uk/78-17VA.pdf, last amended in 2007, http://www.cnil.fr/fileadmin/documents/uk/Decree_No_2005-1309.pdf.

3 World Bank list of "High-income OECD members," online at http://web.worldbank.org/WBSITE/EXTERNAL/DATASTATISTICS/0,,contentMDK:20421402~pagePK:64133150~piPK:64133175~theSitePK:239419,00.html. The OECD (Organization for Economic Cooperation and Development) is a group of nations that subscribe to the "basic values" of "an open market economy, democratic pluralism and respect for human rights." OECD, "Becoming a Member of the OECD: the Accession Process," online at http://www.oecd.org/document/11/0,3343,en_2649_201185_1958091_1_1_1_1,00.html. While Korea does not have a privacy commissioner, it does have a national human rights commission which monitors privacy issues.

4 Emphasis added. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," Article 28; online at http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett or http://tinyurl.com/5owgpa

5 International Covenant on Civil and Political Rights, online at http://www2.ohchr.org/english/law/ccpr.htm.

6 David H. Flaherty, *Protecting Privacy in Surveillance Societies22* (1989), p. 381.

7 In 1967 the Supreme Court finally recognized the right to privacy in telephone conversations in the case Katz v. U.S. (389 US 347), reversing the 1928 opinion Olmstead v. U.S. (277 US 438).

8 The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1897 (1974), codified in part at 5 U.S.C. § 552a, "Records maintained on individuals"; online at http://www4.law.cornell.edu/uscode/uscode05/usc_sec_05_00000552---a000-.html; S. Rep. No. 93-1183 at 1 (1974).

9 U.S. Dept of Housing, Education and Welfare, "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data systems," July 1973; online at http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm.

10 For examples of the abuse of secrecy, see e.g. Alasdair Roberts, *Blacked Out: Government Secrecy in the Information Age* (New York: Cambridge University Press, 2006) .

11 *Walker v. Cheney* , 230 F.Supp.2d. 51 (D.D.C. 2002). Rep. Henry Waxman, a critic of the current situation, issued a statement, "Cheney Task Force Records and GAO Authority," Feb. 12, 2003; online at http://oversight.house.gov/documents/20050203120224-65645.pdf.

12 *Humphrey's Executor v. U.S.*, 295 U.S. 602 (1935). Roosevelt was attempting to remove the commissioner due to policy differences; however, "Any Commissioner may be removed by the President for inefficiency, neglect of duty, or malfeasance in office." Federal Trade Commission Act of 1914 (15 U.S.C §§ 41-58).

13 U.S. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington: GPO, 2004), p. 395. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-408 (2004); Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title VIII, § 801 (2007).

14 See John Solomon and Ellen Nakashima, "White House Edits to Privacy Board's Report Spur Resignation," *Washington Post*, May 15, 2007; online at http://www.washingtonpost.com/wp-dyn/content/article/2007/05/14/AR2007051402198.html. For an overview of the board's short history see Harold C. Relyea, "Privacy and Civil Liberties Oversight Board: New Independent Agency Status," Congressional Research Service, RL34385, updated July 21, 2008; online at http://www.fas.org/sgp/crs/misc/RL34385.pdf.

15 Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53; 121 Stat. 352.

16 Michael Isikoff and Mark Hosenball, "Who's Watching the Spies?" *Newsweek*, July 9, 2008; online at http://www.newsweek.com/id/145140.

17 Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title VIII, § 801(a) (2007)

18 Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title VIII, § 801(a) (2007)

19 Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title VIII, § 801(a) (2007)

20 Douglas Jehl, "Spy Briefings Failed to Meet Legal Test, Lawmakers Say," *New York Times*, Dec. 21, 2005; online at http://www.nytimes.com/2005/12/21/politics/21intel.html.

21 Steve Scherer and Giovanni Salzano, "Italy Halts Online Publication of 2005 Taxpayer Income Figures," Bloomberg .com, April 30, 2008; online at http://www.bloomberg.com/apps/news?pid=20601085&sid=ad2Y2TzEdHKc&refer=europe

22 Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, Title VIII, § 801(a) ''(d) ''(3)

23 Peter Swire, interview. See also "Reflections on the White House Privacy Office," slide presentation, online at http://www.peterswire.net/012908.nc%20state%20b.ppt

24 Ibid.

25 See 5 U.S.C. § 552a(v).

26 See 44 U.S.C. § 3501 note § 208 (the E-Government Act) and 44 U.S.C. §§ 3504(a)(1)(B), (g)(3), 3506(b)(1)(C) (the Paperwork Reduction Act).

27 On OMB's lack of interest and activity on privacy, see for example US Government Accountability Office, "Privacy Act: OMB Leadership Needed to Improve Agency Compliance," GAO-03-304, June 2003; online at http://www.gao.gov/new.items/d03304.pdf

28 President William J. Clinton, *Memorandum for the Heads of Executive Departments and Agencies Regarding Privacy and Personal Information in Federal Records*, May 14, 1998, *available at* http://privacy.navy.mil/presmemo.asp.

29 Office of Mgmt. & Budget, *Memorandum for the Heads of Executive Departments and Agencies Regarding Designation of Senior Agency Officials for Privacy, M-05-08*, Feb. 11, 2005, *available at* http://www.whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf.

30 Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, 2002), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ296.107.

31 Implementing the Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 803, 121. Stat. 266 (2007), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ053.110.

32 Implementing the Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, § 803, 121. Stat. 266 (2007), available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ053.110.

33 These are among the recommendations made by Marc Rotenberg of the Electronic Privacy Information Center in his study "The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11," SSRN WPS (Sept. 2006); online at http://epic.org/epic/ssrn-id933690.pdf. See also Rotenberg, "In Support of a Privacy Protection Agency in the United States," Government Information Quarterly (Winter 1991). For another thoughtful proposal, see Robert Gellman, "A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board," 54 Hastings Law Journal 1183 (2003); online at http://www.bobgellman.com/rg-docs/rg-hastings-2003.pdf.

34 Meanwhile, agency inspector general (IG) offices will also continue to play a part in a multi-layer system of privacy protection. Congress created IG offices within many departments as independent units to audit and investigate agency activities. IGs report to the heads of their agencies but have in many cases operated with a certain degree of independence. In September 2008, Congress passed the Inspector General Reform Act of 1978, which sought to increase the IGs' independence and reduce political interference with their activities. Provisions include a requirement that Congress be notified of the reasons for any removal or transfer of an IG; authorization for IGs to obtain their own counsel, and the establishment of separate budget processes for IG offices. The result is that IG offices can act as a quasi-independent source of privacy oversight as a supplement to agency privacy offices and an overarching independent government data protection authority such as an augmented PCLOB. IG offices are not enough on their own, however. They report to the heads of their agencies and so are not truly independent, and in general their attention to privacy issues has been sporadic. In part this may be because of an inherent conflict: IG offices sometimes find privacy rights make their investigative work more difficult. See Inspector General Act of 1978, , Pub. L. 95-452, Oct. 12, 1978, as amended; Inspector General Reform Act of 2008, , Pub. L. No. 110-409, Oct. 14, 2008; Statement by the President on H.R. 928, the 'Inspector General Reform Act of 2008,'" October 14, 2008; online at http://www.whitehouse.gov/news/releases/2008/10/20081014-7.html.

35 "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," online at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

36 See ACLU, "Surveillance-Industrial Complex," August 2004; online at http://www.aclu.org/FilesPDFs/surveillance_report.pdf.