

26 NOVEMBER 2014

Office of the Director of National Intelligence  
Washington, DC 20511

Mr. John Young  
Cryptome.org  
251 West 89<sup>th</sup> Street  
New York, NY 10024

NOV 24 2014

Reference: ODNI Case # DF-2014-00241

Dear Mr. Young:

This is in response to your 17 June 2014 email to the Office of the Director of National Intelligence (ODNI) (Enclosure 1), in which you requested, under the Freedom of Information Act (FOIA), "a copy of all correspondence with the Intelligence Science Board since its inception in 2002, including requests by ODNI and other agencies for studies currently underway by the Board."

Your request was processed in accordance with the FOIA, 5 U.S.C. § 552, as amended. A thorough search of our records and databases located documents responsive to your request (Enclosure 2).

Information has been withheld pursuant to the following FOIA exemptions:

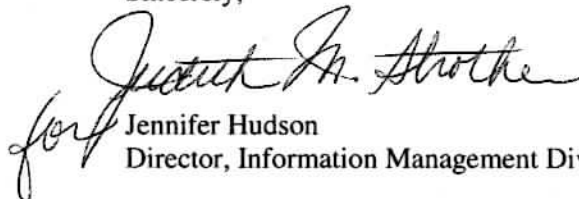
- (b)(3), which applies to information specifically exempt by statutes, specifically, 50 U.S.C. § 3024(m)(1), which protects, among other things, the names and identifying information of ODNI personnel;
- (b)(5), which protects privileged interagency or intra-agency information; and
- (b)(6), which applies to records which, if released, would constitute a clearly unwarranted invasion of the personal privacy of individuals

If you wish to appeal our determination on this request, please explain the basis of your appeal and forward to the address below within 45 days of the date of this letter.

Office of the Director of National Intelligence  
Information Management Office  
Washington, DC 20511

If you have any questions, please email our Requester Service Center at [DNI-FOIA@dni.gov](mailto:DNI-FOIA@dni.gov) or call us at (703) 874-8500.

Sincerely,

  
for Jennifer Hudson  
Director, Information Management Division

Enclosures

DF. 2014-00241

JUN 18 2014

**DNI-FOIA**

---

**From:** John Young <jya@pipeline.com>  
**Sent:** Tuesday, June 17, 2014 1:15 PM  
**To:** DNI-FOIA  
**Subject:** FOIA Request

Office of the Director of National Intelligence Information Management Office Washington, DC 20511

I request a copy of all correspondence with the Intelligence Science Board since its inception in 2002, including requests by ODNI and other agencies for studies currently underway by the Board.

This material will be published on the public education website Cryptome.org.

I agree to pay for costs associated with this request.

Thank you.

Sincerely,

John Young  
Administrator  
Cryptome.org  
251 West 89th Street  
New York, NY 10024  
212-873-8700



**Intelligence Science Board**  
7515 Colshire Drive, McLean, VA 22102

Chair

January 15, 2009

[Redacted]

(b)(6)

Vice Chair

[Redacted]

(b)(3)

Members

[Redacted]

[Redacted]

Dear

[Redacted]

(b)(3)

Enclosed is a summary document highlighting what we consider a topic of fundamental importance to the Intelligence Community (IC): the need for new practices to balance the equally vital imperatives of national security and civil liberties. Many laws and practices that govern intelligence gathering have become anachronistic in the 21st century, where information travels through cyberspace at almost the speed of light, or resides in databanks susceptible to attack or exploitation by our nation's foes. We believe that both privacy and national security would be better served by legal and procedural structures aimed at prohibiting misuse of information rather than restricting acquisition of information, as the Foreign Intelligence Surveillance Act (FISA) does today. Equally important, these new structures must enable the IC to capture intelligence at 21st century speeds – impossible under a FISA process designed to guide 20th century "wiretapping."

While the necessary changes would require action by all branches of the U.S. government, these linked issues are sufficiently urgent that the IC should take steps now to initiate a national dialogue regarding both goals and possible approaches. Therefore, we respectfully request that you bring this document to the attention of the presidential transition team and the incoming Director of National Intelligence. We, and other members of the Intelligence Science Board, will gladly provide further information or assistance in crafting specific proposals to launch productive discussions in this complex and challenging area.

Thank you very much for your consideration.

Best personal regards,

[Redacted]

[Redacted]

(b)(6)

Chair  
Intelligence Science Board

Vice Chair  
Intelligence Science Board

Enclosure

cc:

[Redacted]

(b)(3)

University of Virginia

### **Bringing Intelligence up to Cyber Speed**

The United States must seek to acquire and apply intelligence speedily and effectively enough in cyberspace to better inform decisions and ensuing actions at the tactical, operational, and strategic levels. Technology, policy, and politics all play key roles in enabling or disabling both the intelligence activities needed to identify and counter foreign and domestic threats to the nation and the concomitant means for protecting the privacy of U.S. persons. Both the threats and the protective means rely to various extents on information moving at lightning speeds within the global cyberspace or hiding in increasingly vast data repositories.

---

The very public debate in 2008 over granting immunity to telecommunications carriers for their roles in government intelligence-gathering processes highlighted the unavoidable necessity of tradeoffs between security and privacy. The United States must balance concern for national security – as embodied, for example, in the Constitutional authority of the president as commander in chief – against concern for protecting U.S. persons from unchecked U.S. government power – as spelled out, for example, in the Fourth Amendment’s prohibition of “unreasonable searches and seizures” and its prescription that “no warrants shall issue but upon probable cause.” Thus, the nation must both protect the privacy of U.S. persons who use cyberspace facilities against violations of their Fourth Amendment rights and at the same time allow reasonable and timely intelligence gathering by the U.S. government.

One important but not unique index of the present balance between these sometimes incompatible concerns is the Foreign Intelligence Surveillance Act (FISA). Many believe that the FISA balance adequately accounts for the erosion of the boundaries between the foreign and the domestic within the global cyberspace. However, the undersigned believe that, in practice, the well-intentioned FISA processes actually take place at the scope and speed of retail paper-shuffling in the Industrial Age. Meanwhile, thanks to the 21<sup>st</sup> century Internet and similar technologies, wholesale quantities of data potentially valuable for intelligence purposes will have flashed by at nearly the speed of light. If U.S. intelligence fails to capture these data constellations in transit, they either vanish into the ether forever or else get buried in public and private databanks. These databanks, of ever-expanding scale and scope, have become the targets of the arcane offensive measures and defensive countermeasures characterizing 21<sup>st</sup> century cyber warfare – the current mother of all “wiretapping.” Compounding the difficulty of capturing these sources is the need to reduce the probability of analytic error by ensuring adequate correlation of multiple observable phenomena.

The United States must therefore work out a fresh balance between our equally cherished imperatives of national security and of civil liberties – concepts that are themselves evolving in response to evolving technology, policy, and politics. The real challenge in doing so is to increase and apply the nation’s understanding of these rapidly evolving 21<sup>st</sup> century capabilities and concepts. In the contemporary environment, it seems imperative to generate and evaluate alternative practices that emphasize *prohibiting the misuse of information rather than limiting its acquisition*. Such alternatives might prove more

effective than present practices in both safeguarding civil liberties and improving intelligence collection and analysis. As the U.S. Supreme Court has reminded us repeatedly, "the Constitution is not a suicide pact."

[Redacted]

[Redacted]

**Chairman  
Intelligence Science Board**

[Redacted]

[Redacted]

**Vice Chairman  
Intelligence Science Board**

(b)(6)

June 3, 2009

[Redacted]

(b)(3)

Washington, DC 20511

Dear [Redacted]

(b)(3)

The Intelligence Community (IC) and the Intelligence Science Board (ISB) have long wrestled with how best to balance the needs of national security and intelligence collection with privacy and civil liberty concerns. The enclosed paper by [Redacted] provides an uncommonly lucid and well-reasoned framework for examining the complex and intertwined legal, technical, political, and practical factors at play in striking this balance in today's cyberspace environment.

(b)(6)

I heartily commend [Redacted] paper to you, your staff, and the senior leadership of the IC. **Based on his analysis of the facts available to him, I recommend that you establish an appropriate (perhaps novel) body with the access necessary to form well-grounded conclusions about striking a balance suitable for the 21<sup>st</sup> century. Such a body must necessarily include all three branches of government and, to the extent possible, should also engage the public.**

[Redacted] paper gives us a primer on the technological, legal, policy, and practical constraints associated with intelligence activities in cyberspace. It highlights the debilitating mismatch between the electronic speed of events in cyberspace and the bureaucratic pace of most current IC practices. It then offers a roadmap for addressing these constraints. In particular, [Redacted] argues that the tension between intelligence capacity and privacy is not a zero-sum game – technological advances can be privacy-enhancing even while resulting in more efficient and effective IC capacities.

The paper poses two fundamental questions and a host of ancillary questions, to wit:

1. **Should the legal and political frameworks that restrain IC activities be reformed in light of changing technological and strategic circumstances?** That is,
  - Has the IC *already* sufficiently reoriented from the analog (paper-based) world to the digital era?
  - Do the substantive standards or the sheer logistics imposed by the Foreign Intelligence Surveillance Act (FISA) under some circumstances *in fact* cause the IC to fail to collect important communications?
  - Should the FISA system be modified in order to *automate the process of approving surveillance* as to new targets under certain circumstances in which a FISA order already exists?

- Does the existing system permit the government adequate flexibility to conduct *pattern-based inquiries*, as opposed to inquiries in which it has a specific individual target in mind?
- Do the existing rules employ *categorical distinctions* that no longer make sense, such as a formal distinction between the foreign and domestic realms?
- Do the existing rules employ *technologically contingent* concepts that over time may have become unmoored from their original purpose?
- What are the unappreciated gaps involving *international cooperation* in the realm of information collection and exploitation?
- Are there unwarranted gaps between the formal legal framework(s) that are meant to constrain the IC and the *actual beliefs and practices* that exist within agencies?

**2. If reforms are required, how should they be pursued in order to reflect a reasonable balance between security and privacy values?**

- Would a *general shift toward ex post supervision* (and away from *ex ante* authorization) provide a more satisfactory resolution of the tensions among efficacy, efficiency, and preservation of privacy?
- Can *immutable audit trails* and other forms of accountability-enhancement measures make a switch to post-hoc oversight more attractive from a privacy perspective?
- How can *data-anonymization practices* help to overcome privacy concerns?
- Is the current regime *too complex* to permit adequate training (and therefore more prone to mistakes or abuse)?
- What, if anything, should be done to police the *migration of information* from intelligence uses to other uses, such as criminal law enforcement?

As [redacted] asserts, these questions for the most part turn on empirical facts regarding the actual practice and implementation of status quo rules and practices – facts that are not available to the public and not generally available even within government. While there is good reason for such secrecy, we must not permit reflexive secrecy to prevent vigorous investigation of the issues presented in [redacted] paper.

(b)(6)

Orchestrating a multi-branch (and beyond) body such as the one recommended may be particularly challenging. The ISB and its members have had some experience in dealing with such complex structures. To the extent we can be helpful to you and the IC in characterizing or forming such a body, we stand ready to offer our assistance.

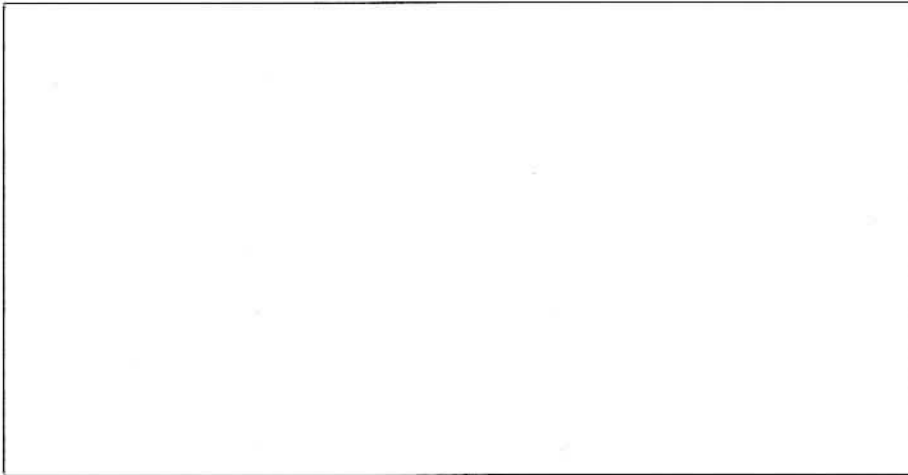
With best regards,

[redacted]
[redacted]

(b)(6)

Enclosure: As stated

cc:



(b)(3)



**Intelligence, Privacy, and the Challenge of Rapid Technological Change:  
Framing the Issues  
Striking a Balance**



(b)(6)

The Intelligence Community (IC) today faces increasing pressure to enhance its ability to collect information in real time, to aggregate and mine that information expeditiously, and at times to do so in contexts where the existence of a threat is known but the particular persons, entities, or facilities associated with that threat are not.<sup>1</sup> Whether the IC can respond appropriately depends in significant part on the hard restraints associated with finite technical capacities. But let us assume for the sake of discussion that existing or emerging technologies are adequate to the task. Two pressing questions arise.

First, would the exploitation of such technologies be compatible with what might best be described as the IC's "regulatory environment"—i.e., the laws, bureaucratic practices and beliefs, and competing policy considerations that collectively function to constrain the IC above and beyond merely technical limitations. Second, if the answer to the first question is no, can and should the regulatory environment be modified? Such questions of course are entangled with privacy and related civil liberty considerations, and appropriately so. Any effort to optimize the IC's use of technology must account for such matters, as recent experience amply demonstrates. It may be, however, that technology can provide Pareto-superior solutions that improve the IC's effectiveness while simultaneously reducing privacy and civil liberty concerns.

This paper does not aspire to answer these ultimate questions. Rather, the goal is to establish that these questions should be rigorously examined, and to provide a roadmap for such an investigation. Toward that end, the paper proceeds in two stages. Part I provides context for the discussion that follows by surveying the evolution of the "regulatory environment" described above. The survey, which follows a historical progression, provides a brief but nuanced account that may be particularly useful for those seeking an accessible introduction to key legal considerations and case studies. Building on that foundation, Part II outlines a research agenda for further study.

**PART I—A PRIMER ON THE LEGAL AND POLICY CONSTRAINTS ASSOCIATED WITH IC  
ACTIVITIES**

We cannot address the challenges described above without a shared understanding of the complex legal and policy considerations that provide the "regulatory environment" for the IC's activities. This section sketches the historical development of those considerations, focusing on IC activities that impact persons in the United States and hence give rise to particular legal and policy concerns.<sup>2</sup>

<sup>1</sup> In terms of the strategic environment, the IC must account not just for the overt threat posed by rival states but also for the threat posed by terrorists and other clandestine actors—a context in which the particular persons and assets to be targeted may not be known even though the threat itself is. At the same time, technological change has produced an increasingly rapid and diversified global communications network as well as exponential growth in the variety and amount of data in existence. These trends oblige the IC to act ever more quickly, and to make use of ever more sophisticated technologies, in order to maintain its edge.

<sup>2</sup> Traditionally, IC activities impacting non-citizens overseas have been understood not to give rise to similar concerns. It bears mentioning that some recent developments in the law, such as the Supreme Court's 2008 decision in *Boumediene v. Bush* (holding that non-citizens held in U.S. military custody at Guantanamo may invoke the Constitution's Suspension Clause), place pressure on that assumption.

## A. From the Founding to 9/11: The Emerging Legal and Political Environment

The current, deeply-contested political and legal climates relating to intelligence activities did not emerge from a vacuum. They are instead the product of a long history involving the evolution of complex and technologically-contingent conceptions of privacy. This section provides a thumbnail sketch of key events in that process, emphasizing the mediating role played by judges.

At common law in England, the primary legal restraint on the investigative powers of government officials was an indirect one: In the event of an unjustifiable intrusion, a government official faced civil liability for trespass. This prospect of course could have a chilling effect if officials were left to predict as best they could how a jury might subsequently evaluate the search. Officials did not have to run such risks, however, thanks to the institution of the judicially-issued search warrant. Obtaining a warrant in advance of a search served not just to protect the private citizen from unwarranted intrusions but also to shield the government agent from the threat of litigation in the event of a close call. The judge, from this point of view, played an *ex ante* mediating role balancing the government's need to investigate with society's interest in preserving some degree of privacy. Not all warrants, however, are equal.

In the period leading up to the American Revolution, the practice of issuing "general" warrants generated fierce resentment from American colonists. General warrants did not specify a particular premises to be searched or a particular item to be seized, but rather purported to grant search and seizure authority (and hence civil immunity) on a generalized basis. This episode, memorialized in American mythos via its inclusion as a prominent grievance in the Declaration of Independence itself, served to entrench the notions that privacy is a central element—perhaps even a precondition—of political liberty and that warrants must be focused narrowly in order to perform their mediating function properly.

The Fourth Amendment proceeds directly from these concerns. It forbids the federal government from engaging in unreasonable searches and seizures. It also specifies that warrants may be issued only where the government can demonstrate "probable cause," with probable cause ordinarily demonstrated to a judicial officer through a sworn statement. The resulting warrants must contain particularized descriptions of the specific places to be searched or items or persons to be seized. The warrant model thus assumes that the government already possesses some amount of information drawing its attention to a particular person or location—an assumption that works reasonably well for the conventional law enforcement scenario, but which encounters problems if applied to, say, an untargeted effort to collect and mine large-scale datasets in search of patterns that might themselves produce more targeted suspicions.

What precisely does the Fourth Amendment mean when it refers to probable cause? The Fourth Amendment does not answer that question explicitly, but the language has long been understood to refer to whether a search will produce evidence that a crime has been or is about to be committed. Not all government investigative activity, however, is directed toward enforcement of criminal law. The government might investigate in furtherance of a public health measure, for example, or to take a more pertinent example, it might collect intelligence in furtherance of its national security and foreign affairs responsibilities (something that I will refer to simply as "intelligence gathering" for ease of reference). And, of course, it might carry out investigations that relate simultaneously to such functions and *also* to criminal law enforcement. Complicating matters further, these interests may not be mutually exclusive (e.g., an espionage or terrorism investigation might sound in both criminal law enforcement and intelligence-

gathering), and even when they are distinguishable their relative weight may shift back and forth in the course of an investigation. These considerations greatly complicate the question of how the Constitution constrains investigative behavior.

These issues were not particularly prominent in the 1800s. A pair of trends that began to accelerate in the 19<sup>th</sup> century ensured, however, that they would become so. First, the revolution in communications technology associated first with steam-powered transportation and then later with the telegraph and the telephone created new opportunities for information collection while at the same time reducing the amount of time required for communications to pass over distance. Second, the emerging role of the United States in international affairs—and the increasingly perilous nature of geostrategic circumstances—increasingly incentivized the federal government to collect information for intelligence purposes. Information had become relatively exigent, in the sense used in this paper, and for much the same reasons. The interesting question was how our legal and political cultures would respond.

The short answer is that both law and politics throughout the 20<sup>th</sup> century oscillated between the concerns of privacy and security, employing categorical distinctions such as geography, purpose and method in order to distinguish zones of relative discretion from zones of relative restraint. These distinctions came under pressure by the end of the century, however, paving the way for the disputes that have characterized the post-9/11 period.

Initially, technological change seemed likely to outstrip the constraining impact of law and politics. In 1928, the Supreme Court in a case called *Olmstead v. United States* addressed whether Fourth Amendment restraints applied to government agents who sought to listen in on phone calls. The question arose in the context of a criminal investigation with no overtones of foreign affairs or national security concerns (the defendants were bootleggers during Prohibition), and it involved activities and communications occurring solely within the United States. The government had tapped the defendants' phones without a warrant, prompting the defendants to object on Fourth Amendment grounds. Drawing a sharp distinction between physically-intrusive measures (such as rifling through a person's papers or invading their home) and the new realm of electronic surveillance, the Court concluded that the Fourth Amendment had no application at all in the latter setting.

The government's victory in *Olmstead* was short-lived. The decision drew the public's attention to the prospect of unregulated wiretapping, generating political backlash. As a consequence, Congress in the 1930s passed a statute criminalizing all wiretapping (though not bugging, which could be viewed as a separate form of collection made possible by changing technology), and by 1940 Attorney General Robert Jackson had forbidden the FBI from employing wiretaps under any circumstances (thus eliminating any concerns regarding the speed with which such operations were conducted, of course). The pendulum, in short, had swung quickly from complete discretion to complete prohibition. But further change quickly followed, largely as a result of World War II.

With the onset of war, the notion of a distinction between criminal investigations and national security investigations became more significant. Not long after Attorney General Jackson forbade the FBI from engaging in wiretapping, in fact, President Roosevelt directed the FBI to conduct extensive investigations of potential national security threats within the United States, including through the use of wiretaps. Privacy protection continued to be robust in the context of mere criminal investigations, but the executive proceeded on the assumption that post-*Olmstead* restraints had no bearing when the purpose of an investigation—even a domestic investigation—involved national security. As a result, the speed with which such investigations

could proceed was left to the discretion of the executive officials involved, subject as always to technical and logistical constraints.

The security-crime distinction soon became an entrenched feature of the legal and political cultures of investigation, at least within the executive branch. Whether the emerging role played by the security-crime distinction also reflected an informed assessment by the public or by Congress, at that time, is a more difficult question. The answer may differ depending on whether we are speaking of investigative activity within the U.S. or abroad. In the latter case, it is fair to say that the public understood that the government engaged in overseas collection activities for security purposes and by and large did not expect those activities to be subject to the sorts of legal and political constraints that might apply domestically. As to the former, however, it is much less clear that the public or members of Congress in the 1950s and 1960s appreciated the nature and scale of the government's domestic security activities.

In any event, change was on the horizon. On one hand, the realm of privacy gave way to a degree in connection with criminal investigations. Pressure on the government to take a tougher line toward crime led Congress, in 1968, to authorize a warrant regime through which the government could obtain permission from a judge to use electronic surveillance for purposes of criminal investigation. On the other hand, the government's discretion to act domestically in the name of security came to an abrupt halt in the early 1970s. While much good had been accomplished through security investigations, many abuses had occurred as well—and these abuses became public knowledge in the 1970s thanks to a combination of investigative journalism and formal investigations conducted by the Senate's Church Committee and the House's Pike Committee. Coming at a time when trust in the government already had collapsed as a result of Vietnam and Watergate—and contemporaneous with growing political interest in the general concept of privacy—these disclosures entrenched a still-influential segment of opinion holding that investigative powers are prone to misuse against political opponents and that the national security establishment accordingly must be subjected to checks and balances in the form of congressional oversight, transparency, statutory regulation, and judicial supervision—at least in its domestic operations.

Given this shift in the political culture, it is little surprise that the legal environment shifted at this time as well. In a case known as the *Keith* decision, the Supreme Court in the early 1970s held that the Fourth Amendment does apply to national security investigations carried out in the U.S. where there the security threat is purely domestic in nature (i.e., where the threat has no tie to a foreign power). The Court did not require the government to employ only criminal investigative methods in such cases—it explicitly stated that the government could satisfy the Fourth Amendment by obtaining a warrant predicated on a showing other than probable cause to believe a crime has been or is going to be committed—but combined with the political blowback discussed above, the net impact was to steer the government towards a criminal law enforcement model of purely domestic security threats.

The security-crime distinction in our legal and political culture thus collapsed, at least to a degree, insofar as purely-domestic security threats were concerned. Insofar as *foreign* security threats were concerned, however, the distinction did not so much collapse as grow more complicated.

In 1978, Congress enacted the Foreign Intelligence Surveillance Act, better known as "FISA." In brief, FISA created a special warrant regime for electronic surveillance directed at agents of foreign powers, with the government's application presented to the Foreign Intelligence Surveillance Court ("FISC") (the membership of which consists of federal judges



picked to serve terms on the FISC by the Chief Justice of the United States). There are several keys to understanding FISA. First, the government's application occurs in a classified setting without any opposing party, and without disclosure to the target then or later (unless and until the government elects to prosecute the target). Second, a FISA warrant does not require probable cause to believe that a crime has been or is going to be committed. Instead, the government's obligation simply is to show probable cause that the target is a foreign power or agent of a foreign power, without respect to any potential crime. In some respects, this may indeed be an easier showing than producing probable cause to believe a crime has been or is going to be committed—though it is worth emphasizing that this still requires a *targeted* showing. Third, the FISA system as framed originally did not apply to *all* or even most foreign intelligence-related surveillance. Instead, FISA offered a complex definition in which the warrant obligation depended on the particular communication technology at issue, the citizenship of the parties to the communication, and the physical location of the parties and of the acquisition device. Generally speaking, this made FISA applicable for wiretaps and bugs employed in the U.S. or in connection with the international communications of U.S. persons, but not for purely extraterritorial communications involving noncitizens. Eventually, FISA expanded to provide for pen registers, trap-and-trace devices, and physical searches as well.

The FISA system, by introducing a formalized gate-keeping process, necessarily imposed temporal delay on the ability of the government to employ covered methods of foreign-intelligence gathering—though the statute has always contained emergency procedures pursuant to which senior Justice Department officials may authorize resort to such methods on a rush basis, subject to post-hoc review from the FISC. Over time, the system grew more complicated. The Justice Department established the Office of Intelligence Policy and Review (OIPR) in order to, among other things, screen and present FISA applications to the FISC. As the system eventually developed, FISA applications ordinarily had to run a gauntlet of internal and external reviews—including first the investigative agency's own general counsel's office, then the OIPR, and finally the FISC itself. FISA does provide emergency procedures through which the Attorney General can approve surveillance on his or her own authority in certain circumstances, subject to FISC approval within seven days. Even then, however, some lapse of time still will occur before the Attorney General can render that approval. The system, in short, necessarily entails some degree of time lapse even in exigent circumstances—a circumstance that would come to be in contrast to the increasing speed with which communications take place in the emerging realm of cyberspace.

Complicating matters, both courts and the Justice Department in the 1980s and 1990s were grappling with the questions that arise when a foreign intelligence investigation might have criminal consequences. Shortly after FISA was enacted, for example, an influential court of appeals decision held that surveillance evidence obtained without a criminal warrant was compatible with the Fourth Amendment only if at the time the "primary purpose" of the investigation was intelligence collection rather than criminal law enforcement; once the primary purpose shifted to the latter, the government must obtain a criminal warrant in order to continue its collection activity. Partially as a result, a "wall" began to emerge in both formal and cultural terms within the executive branch, separating criminal and intelligence investigations so as to reduce the risk of running afoul of the primary purpose test.

In addition to the establishment of the FISA system, the emergence of the "wall," and the collapse of purely domestic security investigations, the revelations of abuse in the 1970s engendered many other pro-privacy developments in our political culture. Perhaps most notably,

advocacy groups oriented toward privacy protection became more numerous and influential. Combined with increasing transparency in government resulting from improved communications technology, public skepticism, the strong post-Watergate emphasis on investigative journalism, and legislative reforms such as the Freedom of Information Act, these groups and other civil liberty/national security watchdog organizations could lobby, litigate, and advocate in favor of regulation and restriction of investigative activity, and often did so quite effectively. One might summarize this development as the institutionalization of the privacy-rights perspective.

Meanwhile, communications technology continued to evolve, and rapidly so. The emergence of the internet and proliferation of online communications—particularly email—presented a profound challenge to many of the categories built in as triggering conditions for the FISA regime. The location of the parties to a communication became more difficult to determine, and perhaps less relevant, as did the location of the acquisition itself. In some instances, the idea of physical location seemed to lose its relevance altogether. The rise of cell phones had a similarly disorienting impact. The location, identity, and status of parties to communications became much harder to ascertain, while at the same time the overall volume of communications expanded dramatically. Making more matters still more problematic, the eventual shift in focus from the threat posed by foreign governments—with their relatively fixed and identifiable personnel and assets—to non-state actors such as al Qaeda increased the importance of intelligence, the difficulty of obtaining it, and the need to obtain it and exploit it as quickly as possible.

## **B. Post-9/11 Developments: Three Case Studies in the Impact of Political and Legal Constraints**

For some observers, the 9/11 attacks (and associated revelations regarding the state of the intelligence community leading up to the attacks) demonstrated both the increasing significance of timely intelligence and the need to ensure that the IC has kept up (and will continue to keep up with) changing communications technology. These events also have drawn attention to the collapse of categorical distinctions that have long played a central role in the law and politics of investigative authority, including the notion of sharp divides between the domestic and the foreign and between crime and security intelligence. For other observers, however, the more salient lessons concern what they perceive to be overreaching by the government in its post-9/11 efforts to reform its investigative powers. The tension between these views is not necessarily insurmountable, but both perspectives have been politicized to an extent that makes reconciliation much more difficult. This section reviews three post-9/11 episodes that amply illustrate this problem, highlighting along the way the current state of the legal and political environment.

### ***1. The USA PATRIOT Act***

In the immediate aftermath of the 9/11 attacks, the Bush Administration advanced an omnibus legislative package that eventually became law as the USA PATRIOT Act. Even prior to its enactment, the PATRIOT Act became a lightning rod for critics who contended that the administration was exploiting the political climate created by the attacks in order to stampede Congress and the public into accepting an array of unnecessary, rights-diminishing measures. Much of the criticism sounded in terms of privacy, reflecting the fact that many of the most controversial measures in the statute tended to expand the government's investigative power:

- “Sneak and peak” search warrants: the PATRIOT Act codified existing caselaw permitting criminal investigators to conduct physical searches pursuant to warrants but without immediate disclosure of the search to the target.
- “Library records”: the PATRIOT Act empowered the FISC to issue orders compelling the production of “any tangible thing” (including, famously, library records) in connection with foreign intelligence investigations, with the recipients of the order forbidden to disclose the existence of the order to others.
- “The wall”: most notably, the PATRIOT Act sought to tear down the criminal-intelligence “wall” by altering the “primary purpose” test. Going forward, investigators could employ FISA so long as foreign intelligence-gathering was a “significant” purpose, even if criminal prosecution was the primary purpose.

These changes met with resistance both from some segments of the public and from some judges. Public resistance culminated, arguably, in a nearly-successful bid to prevent renewal of many of these authorities when they came up for reconsideration in 2004 (the PATRIOT Act had included a “sunset” provision in many instances). The effort to derail or limit renewal failed, but it demonstrated that the privacy lobby is quite well-organized, well-funded, sophisticated, and politically-effective. Legislators going forward would be sensitive to the likelihood that support for a measure raising privacy concerns would generate significant criticism and opposition. As for the judiciary, the FISC initially objected to the effort to lower the criminal-intelligence wall, forcing the government to make the first known appeal to an obscure appellate body known as the Foreign Intelligence Surveillance Court of Review (“FISCR”). Eventually, the FISCR overturned the decision of the FISC, concluding that the “wall” had not been required as a constitutional matter in the first instance (in part because criminal and foreign intelligence investigations are not mutually-exclusive categories) and that the PATRIOT Act settled the question as a statutory matter. Notwithstanding that opinion, however, a federal district judge in Oregon last year reached a contrary conclusion—finding that the Fourth Amendment does compel use of a “primary purpose” test such that the government cannot employ FISA procedures where its primary aim is prosecution—raising the prospect of the wall’s reemergence should the opinion not be reversed on appeal.

## ***2. Total Information Awareness***

No episode better illustrates the perils of underestimating the political salience of privacy concerns than the Total Information Awareness (“TIA”) debacle. In 2002, DARPA consolidated several research programs under the “Information Awareness Office,” with the general aim of cultivating information technologies that would exploit datamining as a means to identify potential terrorists. When the public became aware of the program, it proved deeply controversial. To some extent, this reflected political ham-handedness: Admiral John Poindexter (a figure associated with unlawful executive branch national security actions thanks to his role in the Iran-Contra affair) ran the office, and the very seal of the office (with its all-seeing eye) had Orwellian connotations that played directly into the fears of privacy advocates. But the opposition was not merely a response to cosmetics. TIA increased awareness of a critical change brought about by changing technology. In the past, the limits of technology provided a de facto constraint on the ability of the government (or anyone else, for that matter) to exploit the vast

amount of information about us that arises from our endless exposures to the public world—what some have described as practical anonymity. The existence of practical anonymity in the past had alleviated the need for formal legal constraints on the exploitation of such data, but database technology ensured that practical anonymity was decreasingly effective. The private sector already had made substantial inroads on practical anonymity by the post-9/11 era, of course, but the public by and large had not come to grips with the government's inevitable attempt to follow suit. TIA crystallized the issue in a manner that—fairly or not—conveyed the message that the government was not particularly sensitive to privacy concerns. In February 2003 Congress responded to concerns over TIA by passing legislation suspending IAO operations pending further review, and then in May 2003 by defunding the IAO.

The media have reported that at least some technologies and programs associated with TIA have migrated to other institutional sponsors. Even if true, however, it does not follow that the privacy-based backlash against TIA ultimately was ineffectual. On the contrary, the backlash was sufficiently potent to force Congress at least to appear to denounce the effort, a step which tends to affirm in the public's mind the notion that the effort was indeed inappropriate. Some media reports suggest, moreover, that lingering elements of the program have been sustained in the classified budgets only upon condition that the technologies involved not be employed in connection with U.S. persons. The manifest lesson of the episode, in any event, is that political constraints associated with privacy concerns can be fatal to efforts to exploit technology for informational advantages—at least when handled with inadequate attention to the public's sensibilities on such matters.

### ***3. Warrantless Surveillance and FISA Reform***

The most complex—and most ambiguous—post-9/11 episode involving the interplay of collection, privacy, and technology concerns President Bush's decision to direct NSA to conduct warrantless surveillance within the U.S.—potentially in violation of FISA—and subsequent efforts to reform FISA's triggering conditions. A precise account of these events is beyond the scope of this paper. For present purposes, the following summary suffices:

- After the 9/11 attacks, the President directed NSA to collect international communications coming into or going out of the United States where one party to the communication was linked to al Qaeda or an affiliated terrorist organization—without seeking a FISA order first. The administration reasoned that FISA either did not apply to wartime intelligence gathering, or in the alternative that it could not constitutionally be so applied. Many of the arguments in support of this viewpoint emphasized questions of speed and exigency.
- The existence of the program was leaked to the press, prompting an array of objections and criticisms. Some critics focused on the privacy aspect of the issue, while others were more concerned with the president's implicit claim that as commander-in-chief he could in some circumstances act contrary to statutory commands.
- Allegations that various telecommunication companies had participated in the warrantless surveillance program led to numerous lawsuits seeking potentially-crippling damage awards. This in turn led to a controversial effort in Congress to provide the companies with post-hoc immunity. Recent legislation granted such immunity, though some amount of litigation continues at this time.



- Eventually, the President announced that the surveillance program had been brought within the existing FISA framework. Precisely how this was achieved was not made clear at the time. But whatever agreement had been struck with the FISC initially ultimately broke down, prompting a rushed effort to amend FISA itself.
- FISA has since been amended in a manner that permits the Attorney General and DNI jointly to authorize, for one year's time and without further FISC involvement, the targeting of non-U.S. persons "reasonably believed to be outside the United States," so long as the authorization complies with "minimization" procedures previously approved by the FISC ("minimization procedures" aim to reduce or eliminate incidental and unnecessary collection of the communications of U.S. persons, and to limit retention and dissemination of such communications). The reformed version of FISA also authorizes the AG and DNI to issue such authorization on an emergency basis when necessary (i.e., if the FISC has not already approved minimization procedures and there is no time to seek such approval). In practical terms, the most recent reforms mean that the AG and DNI jointly may draft minimization procedures, have them approved by the FISC for general use, and then issue orders directing collection at specific non-U.S. targets subject to those procedures but without further FISC involvement—including in circumstances that might otherwise have triggered FISA (e.g., a wire communication to or from the United States where the collection will take place in the U.S.).

Like the other episodes discussed above, the FISA reform process—and most certainly the debate regarding the warrantless surveillance program—has demonstrated that Congress is very responsive to privacy concerns, though not to the point of being unwilling to authorize changes to the legal framework governing collection activities that tend to enhance the government's freedom of action. Perhaps the most important lesson to draw from these events is that well-reasoned explanations of why a particular reform is warranted can succeed, though not without substantial opposition from those who feel the government already enjoys authorities that are too robust.

\* \* \*

These post-9/11 vignettes did not directly implicate efforts to increase the speed of intelligence collection, but they nonetheless proved controversial in a manner that serves as a cautionary tale for efforts to reform IC capacities in order to account for the exigent information concern. These post-9/11 changes proved controversial in part because they were portrayed and perceived as enhancing executive branch discretion to determine when and how to gather and use private information. Efforts to reform IC capacities in order to respond to the demands of exigent information are likely to involve a similar move in the direction of relative discretion on the executive's part, and hence we can anticipate similar concerns arising. But it may be that such concerns need not blossom into the full-scale opposition seen in the case studies above. Technology not only motivates and makes possible speed-oriented reforms, but it may also generate new solutions designed to guard against misfeasance and malfeasance—thus ameliorating privacy concerns while improving the IC's efficiency and efficacy

## **PART II – IS REFORM NEEDED? FRAMING A RESEARCH AGENDA**

The events described in Part I make clear that further reform of the IC's capacities would provoke controversy. Some such reform may be necessary, however, in light of the strategic and

technological trends mentioned in the Introduction. The task at hand is to determine—with as much empirical rigor as possible—whether these trends do in fact call for reform.

This Part aims to advance that inquiry by framing a pertinent research agenda. Subpart A begins by specifying a series of general principles and insights (many derived from the events described in Part I), and subpart B concludes with a series of specific questions that ought to be answered in the course of the investigation.

### **A. Background Principles**

- The government's ability to collect and exploit information is constrained and regulated by many factors beyond technological feasibility, including law, bureaucratic culture and practice, policy, and politics. Note that the perception of legal constraints, even if inaccurate, can have a significant impact.
- As technical constraints erode, the question arises whether these other constraints should be enhanced (to preserve the status quo level of protection for privacy in the face of increasing government capacities) or reduced (to permit the government to obtain the full benefit of such increased capacities). Note that some such constraints can have a self-adjusting quality, including a tendency to become more robust when other constraints weaken, in balloon-squeezing fashion. Some, moreover, may be resistant to intentional modification efforts.
- The case for enhancing the IC's capacities in connection with cyberspace and related data-oriented media associated with the modern communications system is strong. Technological change has produced: (i) a vast increase in the volume and variety of potentially-relevant data; (ii) a growing divergence between the speed with which data moves and the amount of time required by non-automated procedures for obtaining ex ante permission for acquisition (whether permission is sought from judges or more senior officials within an organization; and (iii) an increasing need to engage in pattern-based and other relatively untargeted collection and analysis strategies.
- Efforts to reform the IC's capacities in order to account for these trends (i.e., the increasing exigency of information) nonetheless run the risk of encountering significant legal and political opposition, particularly in relation to privacy concerns.
- Privacy is a deeply-entrenched value in our politics and law, but its impact is complex. It provides benefits in that it enriches democratic self-governance—and the social fabric more generally—by preserving space for political dissent and for individual self-definition. It imposes costs insofar as it leads to constraints upon the government's capacity to collect and exploit relevant information for appropriate purposes.
- Where government programs that tend to reduce privacy are handled in a manner that suggests a lack of concern for privacy values, it becomes far easier to characterize them as abusive or potentially abusive and to draw attention away from the potential benefits of such programs. Such opposition can be fatal as a political matter, or at least debilitating. The post-9/11 era is replete with examples, as discussed in Part I.
- Many commentators have observed that the current generation may have a weaker commitment to privacy than past generations, citing the proliferation of private information being displayed openly via social media and the prevalence of private-sector entities engaged in data-collection and aggregation activities. This may be true, but it does not follow that the politics of privacy have changed to the same extent when it

comes to *government* action. A vast amount of personal information—some of it quite sensitive—already finds its way into private hands as a result of technological change, but the public reacts differently—and more negatively—to the same or similar data coming into the government’s possession. This reflects the strength of what we might call the “Big Brother” narrative in our political culture: the view that political liberty depends in part on limiting the government’s access to information about individuals. The phrase “knowledge is power” has positive connotations for some, but disturbing connotations for others—a duality demonstrated by the political firestorm ignited by the Total Information Awareness program.

- The political and legal debate relating to government and privacy often treats the tension between capacity and privacy as a zero-sum game. *It is not clear, however, that it must be so. Technological advances do not necessarily come at the cost of privacy. They can also be privacy-enhancing, even while resulting in more efficient and effective IC capacities.* Anonymous data, immutable audit trails, and similar methods may permit the enhancement of *post-hoc* accountability mechanisms that minimize the risk of abuse or misuse, for example, thus making more tolerable the notion of increased collection and exploitation capacities on the front end.

## **B. Key Questions to Be Answered**

The overarching questions raised by these background considerations are (i) whether the legal and political frameworks that restrain the IC’s activities ought to be reformed in light of changing technological and strategic circumstances, and (ii) whether, if so, such reforms can be designed in a manner that sufficiently accounts for privacy concerns. Both inquiries depend, however, on obtaining well-founded answers to a host of subsidiary questions.

### ***1. Should the legal and political frameworks that restrain IC activities be reformed in light of changing technological and strategic circumstances?***

The IC once operated in a regulatory climate that developed against the backdrop of an analog world (or even a paper-based world). Have we *already* sufficiently reoriented for the digital era? Answering this question requires a comprehensive grasp of the legal frameworks that constrain IC activities, the political realities that sustain those limitations and that have their own direct constraining impact, and—especially—the precise details of how specific programs and policies operate in actual practice. More specifically, one might ask the following questions in the course of such an investigation:

- Do the *substantive* standards imposed by the Foreign Intelligence Surveillance Act (FISA) as a precondition to obtaining a surveillance order from the Foreign Intelligence Surveillance Court (FISC) in some circumstances cause the IC to fail to collect important communications? If so, the question arises whether the substantive standard should be adjusted (and also whether the substantive standard *can* be adjusted, bearing in mind the possibility that a less-restrictive standard might precipitate constitutional objections under the Fourth Amendment).
- Setting aside the substantive standards for obtaining a FISA order, the question also arises whether the sheer *logistics* of obtaining a FISA order might cause the IC to fail to collect important communications. More specifically, one might ask whether

opportunities for collection are missed due simply to the difference in speed between events in cyberspace and the amount of time associated with the non-automated, real-world process of obtaining an order. The existing FISA regime does provide emergency authorization procedures, of course, with the Attorney General having the power to authorize surveillance measures in certain circumstances (subject to an obligation to seek post-hoc approval from the FISC within 7 days). But does the time required to obtain the Attorney General's (or any other person's) permission nonetheless permit some communications to escape collection? Even if the emergency procedures work reasonably well in individual instances, are they sufficiently scalable? If either scenario is a problem, what are the plausible remedies?

- Should the FISA system in any event be modified in order to automate the process of approving surveillance as to new targets in certain circumstances in which a FISA order already exists? For example, assume we have a FISA order in place in connection with a particular foreign target. If that target makes a new contact, should the government automatically have authorization to extend surveillance to that new contact's other communications, subject to post-hoc review and approval?
- How well do the modifications introduced by the Protect America Act, and then by its successor the FISA Amendments Act, respond to these concerns?
- Does the existing system permit the government adequate flexibility to conduct pattern-based inquiries, as opposed to inquiries in which it has a specific individual target in mind? For example, does current law interfere unduly with data-aggregation and -mining solutions by unnecessarily forbidding them, imposing inappropriate political costs in order to pursue them, or simply delaying resort to such tools?
- Do the existing rules employ categorical distinctions that no longer make sense (or as much sense), such as a formal distinction between the foreign and domestic realms? Note, in this regard, that the current FISA regime in many respects depends upon a determination of the physical location of a participant in a communication—a question that technology makes much more difficult to answer in some cases.
- Do the existing rules employ concepts that are technologically-contingent such that over time they become unmoored from their original purpose, covering too much or too little ground?
- Does the increasing difficulty of identifying the parties to a communication, let alone locating them in the physical world, require reform?
- Are there underappreciated gaps or problems involving international cooperation in the realm of information collection and exploitation, perhaps resulting from distinctions between the US approach to data privacy protection and that of other entities (especially but not only the EU)?
- Are there unwarranted gaps between the formal legal framework(s) that are meant to constrain the IC and the actual beliefs and practices that exist within agencies? Are there managerial solutions in place to periodically seek out such gaps, and to take corrective managerial action if so?

***2. If reforms are required, how should they be pursued in order to reflect a reasonable balance between security and privacy values?***

Improving the efficacy and efficiency of the IC's activities does not necessarily require decreased protection for privacy.

- The current regulatory regime often is described as involving *ex ante* authorization rather than *ex post* supervision and oversight. Would a general shift toward the latter provide a Pareto-optimal solution to the tension among efficacy, efficiency, and preservation of privacy?
- Can immutable audit trails and other forms of accountability-enhancement measures make a switch to post-hoc oversight more attractive from a privacy perspective?
- Can data-anonymization practices help to overcome privacy concerns?
- Is the current regime too complex to permit adequate training, such that in actual practice a simplified model would prove less prone to mistakes or abuse even if it appeared on paper to provide fewer restraints?
- What if anything should be done to police the migration of information from intelligence uses to other uses, such as criminal law enforcement or enforcement of the immigration laws? It often is tempting to justify use of a privacy-diminishing method of collection or data-processing by citing the special concerns of the IC, but at the same time one of the most prominent criticisms of the pre-9/11 era was the relative lack of information sharing among agencies. The desire to disseminate information widely, in short, is in tension with the desire to cite special justifications in order to obtain additional authorities.

A concluding thought: These questions for the most part turn on empirical facts regarding the actual practice and implementation of status quo rules and practices, facts that are not available to the public and not generally available even within government. There is good reason for such secrecy as a general proposition, but we must not permit reflexive secrecy prevent vigorous investigation of the issues presented in this paper. An appropriate body can and should be tasked with this inquiry, and can and should be given the access necessary to form appropriately-grounded conclusions.

---