

OVERSIGHT FOR CYBERSECURITY ACTIVITIES*

Why Intelligence Policies Won't Work, and What Kind of Approach Will

Adriane Lapointe

**The opinions expressed in this paper are those of the author alone, and do not reflect the position of any element of the U.S. Government.*

In the absence of consensus on how to balance privacy with the need for government cybersecurity measures, a fallback approach has been to rely on intelligence oversight practices as a possible model for oversight in the cybersecurity realm. A better approach would be to adopt the purely structural aspects of Executive Order 12333, developing a parallel executive order tailored to the distinct goals and operational drivers of cybersecurity. Such a document would establish basic guidelines for policy governing cyber mission, frame cybersecurity privacy issues and goals, and mandate the development of procedures to implement them.

In the context of cybersecurity, as in the context of intelligence, the term “oversight” is frequently used as shorthand for a constellation of issues associated with government monitoring or collection¹ of information associated with U.S. persons². Important though it is, however, oversight (the process of ensuring compliance with some rule set) is cart to the horse of fundamental policy on how information associated with U.S. persons can be used to prosecute cybersecurity mission. Such policy must first determine the extent to which a specific set of cybersecurity activities does or does not compromise network users’ legitimate expectation of privacy, balancing constitutional privacy guarantees (and the more negotiable desire for the greatest possible degree of privacy) with the cost to the

¹ Although national security law related to intelligence does not draw a clear distinction between “collection” and “monitoring” of communications, in a cybersecurity context, the basic dictionary distinction seems appropriate. The term “collect” implies both possession and retention, for however brief a period, while the term monitor suggests purposeful observation of a flow of data (or of any activity), potentially without retention. This paper uses the two terms in this non-legal sense to draw what seems to be a distinction particularly useful in the context of cybersecurity.

² There are of course a variety of ways to define a “U.S. person,” for instance US Federal Code of Regulations, TITLE 22, Chapter 1, §120.15, <http://law.justia.com/us/cfr/title22/22-1.0.1.13.58.0.33.15.html>. The definition of U.S. person that applies to intelligence activities is cited in footnote 5.

nation of failure to ensure some as yet to be determined level of cybersecurity.³ The conclusions drawn would then serve as the basis for decisions about precisely which kinds of data can be monitored, collected, retained, or disseminated, and about the specific cybersecurity purposes for which they can be used. Only after these decisions have been made is it possible to determine how best to ensure both implementation of, and continued compliance with those policies through oversight proper.

To this point, however, it has proven so hard to build consensus on specific policy rules balancing privacy and cybersecurity that we have largely avoided the issue. In such a policy vacuum, individuals with an interest in cybersecurity privacy issues frequently look to *intelligence* oversight, for which both policy and implementing oversight procedures already exist, as a potentially ready-made way to govern cybersecurity mission.

The IC Model of Privacy Policy, Implementation, and Oversight

It's certainly reasonable that anyone thinking about privacy and oversight would begin with a review of the intelligence model. Both Executive Order (E.O.) 12333 and the Foreign Intelligence Surveillance Act (FISA) have been around for a long time, and collection done under these authorities is governed by elaborately articulated (if not always transparent) policies and procedures.

The executive order authorizing intelligence activities, E.O. 12333, "Goals, Direction, Duties, and Responsibilities with Respect to the National Intelligence Effort," outlines IC relationships, describes the specific foreign intelligence mission of each IC entity, and establishes high-level policy on privacy and the handling of U.S. persons (USP) information⁴. The document specifically requires each IC entity to develop procedures to deal with collection, retention, and dissemination of USP data (section 2.3), and to have those procedures approved by the United States Attorney General (AG) and, as of the most recent revision, the Director of National Intelligence. These procedures implement E.O. 12333, in some cases with regard to a specific intelligence discipline, and in others, with regard to the functions of a specific organization. Each IC entity has an oversight and compliance staff and a training regime in place to ensure compliance with the procedures—that is, to ensure both that its workforce and systems minimize the incidental

³ For a highly informed and informative discussion of the cyber threat environment, the issues that need to be addressed if we are to secure our networks, and the urgency of the problem, see William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy" *Foreign Affairs*, September/October, 2010.

⁴ The term U.S. Person includes U.S. corporations here or abroad, and non-citizens resident on U.S. soil, as well as U.S. citizens. For the Intelligence definition of U.S. person, see USC, TITLE 50, Chapter 36, § 180, <http://www.law.cornell.edu/uscode/50/1801.html>.

(inadvertent) collection of U.S. persons information in the course of foreign intelligence collection, and that the agency does not improperly retain or disseminate U.S. persons information. Agencies report quarterly to the AG on any instances in which U.S. persons information was incidentally collected, and on any errors or compliance failures.

Like entities gathering intelligence under E.O. 12333, those doing so under a Foreign Intelligence Surveillance Act (FISA) court order must report to oversight authorities (in this case the FISC—Foreign Intelligence Surveillance Court—as well as the AG) on their compliance with privacy rules.⁵ Unlike E.O. 12333 collection, FISA collection must be explicitly authorized by the FISC because it is known in advance that these special cases involve U.S. persons, and such collection, however clearly justified by national security concerns, would not be allowed under E.O. 12333. The rules for handling of FISA data are dictated by the specific court order under which the intelligence collection takes place. These rules differ from order to order; what can be done with data collected under one FISA certification may be very different from what can be done with comparable data collected under a different certification. For this reason, and because access to FISA data is severely restricted, local oversight of FISA activities is more complex and challenging than that of E.O. 12333 collection.

The Attorney General is responsible for providing integrated information about handling of USP-related information in E.O. 12333 and FISA intelligence activities to Congress.

Why the Policy Informing the IC Model Isn't Right for Cybersecurity: Differences Between Intelligence and Cybersecurity Mission

The E.O. 12333 *structure*—an overarching Executive Order, implementing procedures, and local oversight establishments—would, in a streamlined form, be a reasonable approach for cybersecurity oversight to take; the FISA model is structurally unworkable because of the variability built into its essentially “special case” approach to each new issue.

But the intelligence privacy/oversight *policies* underlying E.O. 12333—that is, the substance of what is being overseen or enforced—are inappropriate for cybersecurity mission because of fundamental differences between the two missions. E.O. 12333 privacy policy and oversight practices were of course developed to address the handling of USP information acquired in the pursuit of foreign intelligence. These procedures are

⁵ Note that the “oversight” addressed in this and the preceding paragraph is operational oversight and handling of USP information rather than top-level Congressional oversight of foreign intelligence activities more generally. <http://uscode.house.gov/download/pls/50C36.txt>.

exceedingly strict because except under very special circumstances, the targets of foreign intelligence (FI) mission must be non-US rather than domestic entities. This means that one goal of intelligence oversight is to ensure that the IC does not stray beyond the limits of its authorized FI mission. Oversight exists as well to deal with the accidental collection of USP information inevitable given the nature of the intelligence activities. We rely on intelligence entities not only to answer explicit, preexisting national security questions, but to identify the broadest possible range of previously unknown threats, conspiracies, plots, etc. But the more widely the IC casts its net, the more likely it is, not only to help thwart terrorist plots, but to catch pieces of USP data that are by law outside the scope of foreign intelligence mission. Recognition of this fact has led to policy, implemented in AG-approved procedures and subject to oversight, that excludes USP data from intelligence collection, analysis, and dissemination, absent a clear link to foreign intelligence⁶.

Cybersecurity is another kind of animal. Although cybersecurity mission also collects, retains, and disseminates information, its purpose and focus, and therefore the nature of its monitoring, its collection activities, and the data it seeks, are both different and by their nature less intrusive. Unlike intelligence activities, which attempt to “connect the dots” across all possible topics, and therefore delve, in a foreign context, into things like message content which would enjoy an expectation of privacy domestically, cybersecurity focuses narrowly on network protection in order to identify, understand, anticipate, and protect against the kinds of threats networks face. These are not the kinds of verbal threats that might be found in the content of an email message, but technical threats like the executable binary (that is, machine-readable) malware that's going along for the ride through the network. While the content of a US person's email message plainly enjoys a right to privacy, no one would suggest that similar protection exists for the malicious code that threatens to compromise our financial transactions, that exposes citizens to the risk of identity theft, that enables the theft of U.S. businesses' intellectual property, and that makes the USG vulnerable to espionage. Beyond the malware itself, most if not all types of data which enable cybersecurity work are already available to every e-commerce or other website any one of us visits, quite independently of whether we make a purchase or sign up for any service; to take the most obvious example, every website knows, or can choose to note, the IP addresses from which it has been contacted.

Perhaps the most important distinction between intelligence and cybersecurity mission is the fact that *routine cybersecurity—as opposed to law enforcement—mission targets malware or malicious activity, not individual people.*⁷ When cybersecurity operatives

⁶ See paragraph 2.3 of E.O. 12333, <https://www.cia.gov/about-cia/eo12333.html#3.2>.

⁷For the purposes of this paper, “routine cybersecurity mission” would be those operational activities involving information sharing across the government for the protection of all federal government systems. Rules governing monitoring, collection, and appropriate use of data on these networks for routine

report that a box has infected another machine on a protected network, the assumption is not that the owner of the source box is a witting participant to the act; in most cases, the domestic (or indeed foreign) box from which malicious traffic is launched onto a government or other network is itself a victim, infected by a bad actor sitting several hops away.⁸ Information linking the individual(s) who may own or use the source box to cyber incidents is relevant to cybersecurity when the box is actually on a government network and victim notification is possible.⁹

Because domestic machines are so easily used by bad actors from around the globe, cybersecurity, unlike intelligence mission, must be as concerned about malicious activity that emerges from a domestic as from a foreign box: domestic botnet zombies are no less pernicious than foreign ones, and it is equally important to protect government networks from both. A study published by computer security firm AVG in August of 2010 concluded that 33% percent of the machines infected by and enlisted into the recent Mumba botnet worldwide were U.S. machines.¹⁰ A 2010 M86 Security Labs assessment claims that 47.39% of all malicious code is hosted in the U.S.¹¹ And in a May 18th, 2010 press release, McAfee stated that “[a]t 98 percent, the United States hosts the majority of new malicious URLs in Q1 2010.”¹²

The bottom line, then, is that if cybersecurity mission is to protect networks from malicious activity, it must be able to monitor networks for anomalous and malicious behavior, identifying the boxes from which malicious activity emanates, whether those machines are

cybersecurity purposes would allow for sharing of information between the managers of networks and incorporation into network security systems. As noted in a later section of this paper, some activities of entities which deal with attribution issues might—or might not—require additional guidance.

⁸ Intelligence, cybersecurity, and indeed law enforcement mission are most likely to overlap in the area of attribution—that is, when an effort is made to trace the ultimate agent back through what is probably a chain of intermediate systems. The greater complexities associated with this kind of work are beyond the routine cybersecurity mission focused on in this paper and can only be touched on here. For an interesting example of both the kind of challenges cybersecurity specialists confront and the role of law enforcement in efforts to attribute malicious activity, see the *Atlantic Monthly's* article on the Conficker worm at <http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/4/>

⁹ Substantive information about the box owner is not a focus of cybersecurity, but cybersecurity alerts could include information about malware propagating itself through messages sent under a co-opted email address which could include an identifiable user name. Inclusion of the email address in threat reporting would allow system administrators to alert their users to delete messages from that address unopened, reducing the amount of cleanup to be done and reducing the spread of infection. How government cybersecurity entities may handle such data—which is, of course, widely circulated in the commercial world—is an example of the kind of policy issue that must be faced squarely and documented.

¹⁰ http://avg.typepad.com/files/revised-mumba-botnet-whitepaper_approved_yi_fv-2.pdf (July, 2010).

¹¹ <http://www.m86security.com/labs/malware-statistics.asp>

¹² http://newsroom.mcafee.com/article_display.cfm?article_id=3650

located across the globe or in my own office in Washington, D.C. While the handling of a US IP address may be appropriately restricted for a U.S. intelligence entity, the ability to identify any and all sources of infection as freely as possible is essential to cybersecurity mission, and policy recognizing that fact and establishing guidelines for it is urgently needed.

At present, in the absence of overarching cyber-specific guidance and procedures, government entities performing cybersecurity functions comply with department-level policy which is derived from E.O. 12333 or which implements the Privacy Act of 1974 or the Electronic Communications Privacy Act (ECPA)¹³. Guidance based on these documents will ensure that privacy rights of U.S. persons are protected, but because none of them was developed with the need to defend networks from malicious activity in mind, that guidance cannot be expected to promote the nation's cybersecurity as well. As already suggested, E.O. 12333 guidance will be far too limiting, and it is unclear whether the terms of the Privacy Act and ECPA even really cover activity in which USP identity is not a focus. Another problem with this rather hodge-podge construct is that rules for the handling of the very same data could vary from one government entity to another. Given the critical importance of the ability to share threat data and indications and warning information in real time, to say nothing of the need to develop a consistent set of rules for automated defensive actions, it is essential that information be handled consistently across the cybersecurity community.

A Tenable Framework for Cybersecurity Privacy Policy and Oversight

We must ask ourselves what exactly it is we need to oversee—that is, what activities we want to protect against when it comes to cybersecurity mission. First, we need to ensure that cybersecurity mission doesn't collect or monitor data types and elements it is not authorized to access—in other words, that it stays within the boundaries set for it. Second, we would want to ensure that cybersecurity mission handles and disseminates legitimately acquired data elements consistent with policy. Oversight would also ensure compliance with the rules telling cybersecurity elements what they can and can't do with USP-associated data—but for the reasons already given, if cybersecurity mission is to succeed, the distinction between USP-associated and all other data will be drawn only for a limited kind of data or for a very narrow set of purposes. It is essential that we establish

¹³ 5 U.S.C. 552a. <http://thomas.loc.gov/cgi-bin/bdquery/z?d093:SN03418:@@L&summ2=m&>. Although it applies more widely in some cases, the Privacy Act was designed to ensure that government entities which have a legitimate reason to incorporate USP-associated information into databases that can be searched by personal identifier do so in a transparent and accountable fashion. The Electronic Communications Privacy Act, 18 U.S.C. 119, is focused on interception of content http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_120_119.html.

the underlying policy and procedures with which we expect compliance if we are to avoid an inconsistent, accreted rather than rationally planned set of processes for cybersecurity.

Although the intelligence and cybersecurity missions are very different and the policy that governs them must differ as well, aspects of the E.O. 12333 *structure* could be of real use in the establishment of cybersecurity privacy and oversight policy. A cybersecurity executive order structured like the generally quite readable E.O. 12333 would identify executive branch cybersecurity players and enumerate their authorities and missions¹⁴. It would provide high-level policy guidance on the handling and sharing of USP-associated data reflective of the need to monitor networks, collect malware and related data, and make appropriately delimited use of the kind of information that cybersecurity, as distinct from intelligence, requires if its practitioners are to defend networks and protect the citizens who use them.

Specifically, a cyber executive order would:

1. Provide high-level policy guidance recognizing the need both to protect Fourth Amendment Privacy rights, and to protect USG networks from malicious activity.
2. State the President's intent on the sharing of cyber threat information including selected kinds of data associated with USPs, with state, local, and tribal entities, and with the private sector.¹⁵
3. Identify an executive agent for cybersecurity privacy and oversight policy, and charge that entity with development of policy on the handling and sharing of USP-associated data that reflects the need to monitor networks, collect malware and related data, and make appropriately delimited use of the kind of information that cybersecurity requires if its practitioners are to defend networks and protect the citizens who use them.

Among the named responsibilities of the Executive Agent would be to:

1. Serve as the chair of a committee composed of a limited number of technical, legal/policy, and privacy experts from across the cybersecurity community charged with
 - Identifying those data types essential to cybersecurity mission;

¹⁴ Currently the only policy assigning specific roles and responsibilities in cyber is NSPD 54/HSPD 23, "The Comprehensive National Cybersecurity Initiative." But as this document is both highly classified and closely held, even the very general guidance it provides has had less operational impact than might have been desired.

¹⁵ Subsequent policy and oversight in this area would of course govern only the dissemination of cybersecurity information by the USG entities over which the executive order has authority.

- Identifying how each data type is used;
- Determining, in collaboration with the Department of Justice, which of these data types might enjoy an expectation of privacy and under what circumstances;
- Weighing, for final decision by the executive agent, any negotiable conflicts between privacy and cybersecurity risk; and once that decision has been made,
- Developing the shortest possible overarching document describing the uses that may be made of each relevant data type for use throughout the cybersecurity community and establishing the underlying principles of the decisions made.

2. Reconvene this or a similar committee on a regular basis to review any privacy policy challenges presented by new technologies and new data types, and make decisions on the handling of such data.¹⁶

3. Direct each USG cybersecurity entity to develop procedures for the conduct and oversight of cybersecurity mission consistent with these common data-handling rules and reflecting that entity's specific cyber mission. These procedures would be approved at a minimum by the Executive Agent. It would be highly desirable if these procedures were written as explicit user manuals for cybersecurity personnel, not as arcane legal documents requiring the agencies to provide an additional layer of interpretation.

In mandating the development of more specific policy, this cybersecurity executive order might consider a distinction between categories of cybersecurity mission for which privacy rules and oversight will be more or less complex. The largest category could be what this paper has referred to as "routine" cybersecurity mission, those operational activities involving information sharing across the government for the protection of all federal government systems. Rules governing monitoring, collection, and appropriate use of data on these networks for routine cybersecurity purposes would allow for sharing of information between the managers of networks and incorporation into network security systems. These should be the most basic decisions, those with the greatest ramifications, and also those that should be made most quickly.

It's possible that some additional policy might apply to a smaller, "Tier One" category including such entities as the cyber centers identified in NSPD 54/HSPD 23. The centers are charged with more than the protection of their own organization's networks, and do work including malware analysis, computer forensics, attribution research, and dynamic

¹⁶ The obvious danger here is micromanagement of mission by a far-distant and high-level committee, and this must be avoided. But slow response time to significant changes in technology which clearly fall outside existing guidance is a real problem. It's also true that such a committee can only remain informed if it is exposed sufficiently often to the operational world it exists to oversee and support.

defense. Some of them also interface with law enforcement and the IC. Some of these activities might give rise to privacy concerns distinct from those of routine cybersecurity mission.

Conclusion

An Executive Order for cybersecurity must meet two challenges in its treatment of privacy policy and oversight. It must ensure political transparency by identifying a widely-trusted executive agent and giving that agent sufficient authority and funding to execute its assigned mission—which must include providing information about the oversight process to the public. It must also support operations by ensuring that the specific oversight processes developed support the cybersecurity goals codified in policy, that they are as streamlined and as little bureaucratic as possible, and that they are subject to modification through a clearly and publicly articulated process when changes in technology make procedural change appropriate.

As any wise oversight officer knows, before you institute an oversight regime, you'd better know exactly what you need to protect against. If we acknowledge that cybersecurity is different from intelligence, we will be better prepared to assess realistically the privacy impact of cybersecurity measures and to take mission-appropriate actions to ensure privacy protection when we need to do so. An executive order for cybersecurity would be a good way to draw the distinction and move us toward the cyber-specific policy we need.



As this paper was in its final stages, the assault of the Stuxnet worm on Iranian nuclear (and non-nuclear Pakistani, Indian, and Indonesian) sites was making news around the globe and bringing home to anyone who followed the story the importance of cybersecurity for U.S. networks. Based on its level of sophistication, most experts in the press attributed the worm to a nation-state, citing variously the governments of the U.S., Israel, the UK, France, China, and Russia as possible sources. Although it is not clear at this time whether the worm is in fact responsible for delays in Iran's developing nuclear program, most, though not all, experts believe that this was the worm's intent.¹⁷

¹⁷ David E. Sanger, "Iran Fights Malware Attacking Computers." <https://www.nytimes.com/2010/09/26/world/middleeast/26iran.html> ; Robert McMillan, "Was Stuxnet Built to Attack Iran's Nuclear Program?"; http://www.pcworld.com/businesscenter/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html; Arthur Bright, "Clues Emerge About Genesis of Stuxnet Worm."

Commentators described Stuxnet as “the first such attack on [a] critical industrial infrastructure that sits at the foundation of modern economies.”¹⁸ The Stuxnet worm is not only an example of the danger sophisticated malware poses to infrastructure specifically and government projects generally, but a likely instigation to future targeted malware attacks: quite apart from which nation, if any, actually bears responsibility for the Stuxnet worm, any nation *suspected* of involvement is a target for malware reprisals that seem likely to fly. That list obviously includes the U.S. The sooner we act to address privacy concerns and establish cybersecurity data-handling policy, the sooner we will be able to protect ourselves more fully from both the direct and indirect damage that could be caused by the next Stuxnet.

<http://www.csmonitor.com/World/terrorism-security/2010/1001/Clues-emerge-about-genesis-of-Stuxnet-worm>

¹⁸ Riva Richmond, “Malware Hits Computerized Industrial Equipment.”

<http://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/>