Your on the Street Reporter

Uyless Black

The President's Review Group Findings

President's Review Group on Intelligence and Communications Technologies

April 6, 2014

Hello from Your on the Street Reporter. This report continues the series on Internet privacy and security specifically, and privacy and security in America generally. The focus of this essay is the President's Review Group on Intelligence and Communications Technologies, released December 12, 2013. (Also referred to as the "Group" in this report.) I have delayed posting information on this report. I thought some background essays would be helpful in interpreting the suppositions, findings, and recommendations in this document.

The report is 308 pages, containing forty-six recommendations. My intent in this posting is to summarize the highlights and main points of the report. An addendum provides a summary of the recommendations.

I was surprised by some of the points made by this group. One that caught my eye was their view of security. The group contends that personal privacy is a form of security, an idea I have not seen expressed in this way:

> ***The United States Government must protect, at once, two different forms of security: national security and personal privacy*.**
> In the American tradition, the word "security" has had multiple meanings. In contemporary parlance, it often refers to *national security* or *homeland security*. One of the government's most fundamental responsibilities is to protect this form of security, broadly understood. At the same time, the idea of security refers to a quite different and equally fundamental value, captured in the Fourth Amendment to the United States Constitution: "The right of the people to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . " (emphasis added). Both forms of security must be protected.

The concepts expressed in this brief passage are illustrative of many debates taking place in America today and high-lighted in this series of essays. (Especially expressed in Report IX, "Where is the Line Drawn?"). I extract a short piece from my report to set the stage for the remainder of this narrative:

> In an earlier report posted on this blog, I made reference to someone who claimed that modern citizenry in a democratic, republican nation can have both security and privacy. To a degree, yes, but not complete security and complete privacy. In the 21st century, we must come to understand that where one gains the other loses.

> But it need not be to an extreme of compromising, much less abandoning, the bedrocks of America's democratic and republican underpinnings. Else, what is the point?

Given these ideas, I am heartened by the President's Review Group on Intelligence and Communications Technologies assertions and recommendations. The Group poses solutions to the current problem, ones that I think cross the red and blue boundaries of America's politics. I have paraphrased below several assertions and recommendations that relate to contentions I have made in the essays in this series. The text below is paraphrased from this report. I have added comments that are contained within brackets.

- Excessive surveillance and unjustified secrecy can threaten civil liberties, public trust, and the core processes of democratic self-government.

- Because America's adversaries operate through the use of complex communications technologies, the National Security Agency, with its impressive capabilities and talented officers, is indispensable to keeping our country and our allies safe and secure.

- The US Government should fully support and not undermine efforts to create encryption standards. It will not in any way subvert, undermine, weaken, or make vulnerable generally available commercial encryption. It should support efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage. [I cannot help but think agencies, such as the FBI, CIA, and NSA, will find this pill hard to swallow. I might, too, if I were in their shoes. But I am not, and hope we citizens can be confident that our email will be as sacrosanct as our letter within a postal service envelope.]

- [I have expressed concern about the emerging Orwellian threats Uncle Sam can make to private parties to release information they have promised to hold in trust for their customers] Restrictions should be placed on the ability of the Foreign Intelligence Surveillance Court (FISC) to compel third parties (such as telephone service providers) to disclose private information to the government; with similar restrictions on the issuance of National Security Letters (by which the Federal Bureau of Investigation now compels individuals and organizations to turn over certain otherwise private records).

- [In these reports, I have lobbied for America's intelligence surveillance systems to be subject to a rigorous cost/benefit analysis, not unlike private industry does routinely on its programs: a track record, if you will.] Legislation should be enacted requiring information about surveillance programs to be made available to the Congress and to the American people to the greatest extent possible (subject only to the need to protect classified information). [Further, Recommendation 46:] "We recommend the use of cost-benefit analysis and risk management approaches, both prospective and retrospective, to orient judgments about personnel security and network security measures."

- [I have also lobbied for an ombudsman who can act as a brake on what will always be excesses (in any organization with few reins.)] With respect to the FISC, Congress should create the position of Public Interest Advocate to represent the interests of privacy and civil

> liberties before the FISC. We also recommend that the government should take steps to increase the transparency of the FISC's decisions and that Congress should change the process by which judges are appointed to the FISC.

As I mentioned above, I am encouraged by the opinions, findings, assertions, and recommendations of the panel. Their proposals do not severely curtail the current activities of America's intelligence/surveillance system. They do (a) make them more accountable, (b) more transparent (to properly designated parties), and (c) rein-in what are becoming disturbing breeches of the Fourth Amendment.

Addendum
Recommendations of the President's Review Group on Intelligence and Communications Technologies

Almost all the text in this addendum is paraphrased from the original report. I have omited a lot of it, and added some comments (italicized and in brackets). I recommend you read this material. It will give you a firm understanding of how shaky the foundations are for protecting Fourth Amendment rights and how these recommendations go a long way in repairing these foundations.

Recommendation 1: Section 215 *[Section 215 is read to mean any "tangible thing," including business records, for national security purposes*.] should be amended to authorize the Foreign Intelligence Surveillance Court to issue a section 215 order compelling a third party to disclose otherwise private information about particular individuals only if: (1) it finds that the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect "against international terrorism or clandestine intelligence activities" and (2) like a subpoena, the order is reasonable in focus, scope, and breadth.[*The idea behind the recommendation is that is gives FBI, etc too much discretionary power. So, the FISC would act as arbiter.]*

Recommendation 2: Statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that: (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect "against international terrorism or clandestine intelligence activities" and (2) like a subpoena, the order is reasonable in focus, scope, and breadth. [*A national security letter (NSL) is an administrative subpoena issued by the Federal Bureau of Investigation (FBI). Administrative subpoenas are authorized by many federal statutes and may be issued by most federal agencies. Most statutes authorizing administrative subpoenas authorize an agency to require the production of certain records for civil rather than criminal matters.*]

Recommendation 3: All statutes authorizing the use of National Security Letters should be amended to require the use of the same Oversight, minimization, retention, and dissemination standards that currently govern the use of section 215 orders. [*Again, a curtailment to "going-it-alone."*]

[*This recommendation is quite important. The text below is a good example for how the Law of Creeping Momentum leads to government overuse and abuse:]*

When NSLs were first created, the FBI was empowered to issue an NSL only if it was authorized by an official with the rank of Deputy Assistant Director or higher in the Bureau's headquarters and if it were deemed of the utmost importance. The PATRIOT Act of 2001 significantly expanded the FBI's authority to issue NSLs. **First**, the PATRIOT Act authorized every Special Agent in Charge of any of the Bureau's 56 field offices around the country to issue NSLs. **Second**, the PATRIOT Act eliminated the need for any *particularized* showing of individualized suspicion. Under the PATRIOT Act, the FBI can issue an NSL whenever an authorized FBI

official certifies that the records sought are "relevant to an authorized investigation." **Third**, the PATRIOT Act empowered the FBI to issue nondisclosure orders (sometimes referred to as "gag orders") that prohibit individuals and institutions served with NSLs from disclosing that fact, and it provided for the first time for judicial enforcement of those nondisclosure orders. In contemplating the power granted to the FBI in the use of NSLs, it is important to emphasize that NSLs are issued directly by the FBI itself, rather than by a judge or by a prosecutor acting under the auspices of a grand jury. Courts ordinarily enter the picture only if the recipient of an NSL affirmatively challenges its legality.

NSLs have been highly controversial. This is so for several reasons. **First**, as already noted, NSLs are issued by FBI officials rather than by a judge or by a prosecutor in the context of a grand jury investigation. **Second**, as noted, the standard the FBI must meet for issuing NSLs is very low. **Third**, there have been serious compliance issues in the use of NSLs. In 2007, the Department of Justice's Office of the Inspector General detailed extensive misuse of the NSL authority, including the issuance of NSLs without the approval of a properly designated official and the use of NSLs in investigations for which they had not been authorized. Moreover, in 2008, the Inspector General disclosed that the FBI had "issued [NSLs] after the FISA Court, citing First Amendment concerns, had twice declined to sign Section 215 orders in the same investigation." **Fourth**, the oversight and minimization requirements governing the use of NSLs are much less rigorous than those imposed in the use of section 215 orders. **Fifth**, nondisclosure orders, which are used with 97percent of all NSLs, interfere with individual freedom and with First Amendment rights.

[*I challenge even the most pro-surveillance zealots on this planet to defend how these actions do not constitute serious intrusions into the civil liberties of American citizens*.]

Recommendation 4: As a general rule, and without senior policy review, the government should not be permitted to collect and store all mass, undigested, non-public personal information about individuals to enable future queries and data-mining for foreign intelligence purposes. Any program involving government collection or storage of such data must be narrowly tailored to serve an important government interest. [*If someone else has the world's metadata in storage, what's the difference? Uncle Sam can go after it. True, but only (if these recommendations are put into place) after proper authorization has been made*.]

Recommendation 5: Legislation should be enacted that terminates the storage of bulk telephony meta-data by the government under section 215, and transitions as soon as reasonably possible to a system in which such meta-data is held instead either by private providers or by a private third party. Access to such data should be permitted only with a section 215 order from the Foreign Intelligence Surveillance Court that meets the requirements set forth in Recommendation 1.

Recommendation 6: The government should commission a study of the legal and policy options for assessing the distinction between metadata and other types of information. The study should include technological experts and persons with a diverse range of perspectives, including experts about the missions of intelligence and law enforcement agencies and about privacy and civil

liberties. [*This series introduces this subject. I have more detailed information that given time, I will share with you (and the President's group…if they bother to read my blog*.]

Recommendation 7: Legislation should be enacted requiring that detailed information about authorities such as those involving [programs discussed in these series, such as NSA surveillance, National Security Letters, etc.] should be made available on a regular basis to Congress and the American people to the greatest extent possible, consistent with the need to protect classified information. With respect to authorities and programs whose existence is unclassified, there should be a strong presumption of transparency to enable the American people and their elected representatives independently to assess the merits of the programs for themselves. [*I cannot imagine the intelligence community not going to the mat to prevent this level of transparency. They will claim we are giving away the company store to the terrorists. Maybe. Two scenarios exist, (both in satire, to give us a break.) (A) Or maybe we would be giving away the company store about how effective the programs are that all terrorists will renounce terrorism and convert to democracy and Christianity. (B) Or maybe it would demonstrate how ineffective the programs are that Americans would cancel many programs and fire many intelligence gurus.*]

Recommendation 8: [*Some details on nondisclosure, not pertinent to this report.]*

Recommendation 9: [*Some details on nondisclosure, not pertinent to this report.]*

Recommendation 10: [*Some details on nondisclosure, not pertinent to this report.]*

Recommendation 11: The decision to keep secret from the American people programs of the magnitude of the section 215 bulk telephony meta-data program should be made only after careful deliberation at high levels of government and only with due consideration of and respect for the strong presumption of transparency that is central to democratic governance. [*Again, an idea that will be contested by the intelligence community*.]

Recommendation 12: [*When I first read Recommendation 12, I thought the group would be hamstringing our Intelligence services from associating nefarious citizens with nefarious non-citizens. Upon several readings, I over reacted. This recommendation simply requires less seat-of-the-pants surveillance of citizens.*] If the government legally intercepts a communication that justifies the interception of a communication on the ground that it is directed at a non-United States person who is located outside the United States, and if the communication either includes a United States person as a participant or reveals information about a United States person: (1) any information about that United States person should be purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others;(2) any information about the United States person may not be used in evidence in any proceeding against that United States person;(3) the government may not search the contents of communications in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism

Recommendation 13: [*Amplifies aspects of Recommendation 12 not pertinent to this report.]*

Recommendation 14: [*Suggests using some Department of Homeland Security procedures on privacy issues.*]

Recommendation 15: The National Security Agency should have a limited statutory emergency authority to continue to track known targets of counterterrorism surveillance when they first enter the United States, until the Foreign Intelligence Surveillance Court has time to issue an order authorizing continuing surveillance inside the United States. [*This rule should encourage all parties to get off their duffs and move things along*.]

Recommendation 16: [*A recommendation on approving (at a high level) sensitive operations (as one example: tapping telephone lines of world leaders.]*

Recommendation 17: [*A recommendation on having higher level officials involved in certain activities.]*

Recommendation 18: The Director of National Intelligence should establish a mechanism to monitor the collection and dissemination activities of the Intelligence Community to ensure they are consistent with the determinations of senior policymakers.

Recommendation 19: [*This recommendation urges Uncle Sam's intelligence community to be careful and debate fully the spying on foreign leaders. This action should be approved only at the highest levels government.*]

Recommendation 20: The US Government should examine the feasibility of creating software that would allow the National Security Agency and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection. *[I have some initial ideas about this recommendation that I will develop more fully and share with you later.*]

Recommendation 21: A small number of closely allied governments, meeting specific criteria, the US Government should explore understandings or arrangements regarding intelligence collection guidelines and practices with respect to each others' citizens (including, if and where appropriate, intentions, strictures, or limitations with respect to collections).

Recommendation 22: The Director of the National Security Agency should be a Senate-confirmed position. Civilians should be eligible to hold that position. The President should give serious consideration to making the next Director of the National Security Agency a civilian. [*The group has nothing further to say on this matter.]*

Recommendation 23: The National Security Agency should be clearly designated as a foreign intelligence organization. Missions other than foreign intelligence collection should generally be reassigned elsewhere. [*This recommendation makes no sense to this writer. How can an intelligence organization function if it does not collect information?]*

Recommendation 24: The head of the military unit, US Cyber Command, and the Director of the National Security Agency should not be a single official.

Recommendation 25: The Information Assurance Directorate—a large component of the National Security Agency that is not engaged in activities related to foreign intelligence—should become a separate agency within the Department of Defense, reporting to the cyber policy element within the Office of the Secretary of Defense.

Recommendation 26: There should be a privacy and civil liberties policy official, located both in the National Security Staff and the Office of Management and Budget.

Recommendation 27: The charter of the Privacy and Civil Liberties Oversight Board should be modified to create a new and strengthened agency, the Civil Liberties and Privacy Protection Board, that can oversee Intelligence Community activities for foreign intelligence purposes, rather than only for counterterrorism purposes. The Civil Liberties and Privacy Protection Board should be an authorized recipient for whistle-blower complaints related to privacy and civil liberties concerns from employees in the Intelligence Community. An Office of Technology Assessment should be created within the Civil Liberties and Privacy Protection Board to assess Intelligence Community technology initiatives and support privacy-enhancing technologies. Some compliance functions, similar to outside auditor functions in corporations, should be shifted from the National Security Agency and perhaps other intelligence agencies to the Civil Liberties and Privacy Protection Board. [*It's the old saw: If an organization does not police itself, if it does not stay in touch with ongoing events and preferences in the real world, Uncle Sam will step in and generally yield an overkill hammer to the problem. Time and again, organizations muck-up their charter, and government imposes yet more restrictions and overhead to their operations*.]

Recommendation 28: Congress should create the position of Public Interest Advocate to represent privacy and civil liberties interests before the Foreign Intelligence Surveillance Court. [*As you know, I have been lobbying for this position in several essays in this series.]*

Recommendation 29: The US Government should: (1) fully support and not undermine efforts to create encryption standards; (2) not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software; and (3) increase the use of encryption and urge US companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage. [*I would add that a secure entity in the government be granted access to CIA, DIA, NSA, etc. deciphering technologies to determine if these agencies are indeed adhering to this potential law. I don't trust any organization to police itself. I regret having to make this statement, but I've been around too many curves in the road to believe bureaucratic straight-shooters are the exception and not the rule.*]

Recommendation 30: The National Security Council staff should manage an interagency process to review on a regular basis the activities of the US Government regarding attacks that exploit a previously unknown vulnerability in a computer application or system. These are

often called “Zero Day” attacks because developers have had zero days to address and patch the vulnerability. US policy should generally move to ensure that Zero Days are quickly blocked, so that the underlying vulnerabilities are patched on US Government and other networks.

Recommendation 31: The United States should support international norms or international agreements for specific measures that will increase confidence in the security of online communications.

Recommendation 32: There should be an Assistant Secretary of State to lead diplomacy of international information technology issues.

Recommendation 33: As part of its diplomatic agenda on international information technology issues, the United States should advocate for, and explain its rationale for, a model of Internet governance that is inclusive of all appropriate stakeholders, not just governments.

Recommendation 34: The US Government should streamline the process for lawful international requests to obtain electronic communications through the Mutual Legal Assistance Treaty process.

Recommendation 35: For big data and data-mining programs directed at communications, the US Government should develop Privacy and Civil Liberties Impact Assessments to ensure that such efforts are statistically reliable, cost-effective, and protective of privacy and civil liberties.

Recommendation 36: For future developments in communications technology, the US should create program-by-program reviews informed by expert technologists, to assess and respond to emerging privacy and civil liberties issues, through the Civil Liberties and Privacy Protection Board or other agencies.

Recommendation 37: The US Government should move toward a system in which background investigations relating to the vetting of personnel for security clearance are performed solely by US Government employees or by a non-profit, private sector corporation. [*Granted, I am long since removed from working in intelligence, but I cannot imagine why the US Government would do otherwise.*]

Recommendation 38: The vetting of personnel for access to classified information should be ongoing, rather than periodic. A standard of Personnel Continuous Monitoring should be adopted, incorporating data from Insider Threat programs and from commercially available sources, to note such things as changes in credit ratings or any arrests or court proceedings. [*Whew. This recommendation appears harmless enough, and if enacted in the past, might have caught Ames and others. But it could lead to an Orwellian bureaucracy.]*

Recommendation 39: Security clearances should be more highly differentiated, including the creation of “administrative access” clearances that allow for support and information technology personnel to have the access they need without granting them unnecessary access to substantive policy or intelligence material.

Recommendation 40: The US Government should institute a demonstration project in which personnel with security clearances would be given an Access Score, based upon the sensitivity of the information to which they have access and the number and sensitivity of Special Access Programs and Compartmented Material clearances they have. Such an Access Score should be periodically updated.

Recommendation 41: The "need-to-share" or "need-to-know" models should be replaced with a Work-Related Access model, which would ensure that all personnel whose role requires access to specific information have such access, without making the data more generally available to cleared personnel who are merely interested. [*Need to know and need to share do not include people who are merely interested. I find this recommendation disturbing, as it assumes there are far too many casual readers of classified information.*]

Recommendation 42: The Government networks carrying Secret and higher classification information should use the best available cyber security hardware, software, and procedural protections against both external and internal threats. The National Security Advisor and the Director of the Office of Management and Budget should annually report to the President on the implementation of this standard.[*It is reasonable to ask why this recommendation is even needed?*]

Recommendation 43: The President's prior directions to improve the security of classified networks, Executive Order 13587, should be fully implemented as soon as possible.

Recommendation 44: The National Security Council Principals Committee should annually meet to review the state of security of US Government networks carrying classified information, programs to improve such security, and evolving threats to such networks. An interagency "Red Team" should report annually to the Principals with an independent, "second opinion" on the state of security of the classified information networks. [*This is a recommendation that should not have to be made. It should have already been part of a procedure*.]

Recommendation 45: All US agencies and departments with classified information should expand their use of software, hardware, and procedures that limit access to documents and data to those specifically authorized to have access to them. [*This recommendation is related to Recommendation 41. Again, I am dumbfounded as to why this group believed it had to state the obvious. If relevant, it demonstrates monumental incompetency of America's intelligence gurus.]*

Recommendation 46: Use cost-benefit analysis and risk management approaches, both prospective and retrospective, to orient judgments about personnel security and network security measures. [*Another welcome recommendation*.]