NEW AMERICA

CYBERSECURITY INITIATIVE

New America Cybersecurity Fellows Paper Series - Number 1

THE DECLINING HALF -LIFE OF SECRETS

And the Future of Signals Intelligence

By Peter Swire

July 2015

ABOUT THE AUTHOR
Peter Swire, Nancy J. and Lawrence P. Huang Professor of Law and Ethics, Scheller College of Business, Georgia Institute of Technology; Senior Counsel, Alston & Bird LLP; and New America Cybersecurity Fellow

ABOUT THE CYBERSECURITY INITIATIVE
The Internet has connected us. Yet the policies and debates that surround the security of our networks are too often disconnected, disjointed, and stuck in an unsuccessful status quo. This is what New America's Cybersecurity Initiative is designed to address. Working across our International Security Program and the Open Technology Institute, we believe that it takes a wider network to face the multitude of diverse security issues. We engage across organizations, issue areas, professional fields, and business sectors. And through events, writing and research, our aim is to help improve

ACKNOWLEDGEMENTS
Many thanks to Ross Anderson, Ashkan Soltani and Lee Tien for assistance with this draft, and to the fellow members and staff of the President's Review Group on Intelligence and Communication Technology, where many of these ideas were developed. This paper represents the author's views, and not the views of other members of the Review Group.

PHOTO CREDIT COVER PHOTO - Shutterstock

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The nature of secrets is changing. Secrets that would once have survived the 25 or 50 year test of time are more and more prone to leaks. The declining half-life of secrets has implications for the intelligence community and other secretive agencies, as they must now wrestle with new challenges posed by the transformative power of information technology innovation as well as the changing methods and targets of intelligence collection.

This Page Left Intentionally Blank

INTRODUCTION: THE CHANGING NATURE OF SECRETS

The nature of secrets is changing. The "half-life of secrets" is declining sharply for many signals intelligence and other intelligence activities as secrets that may have been kept successfully for 25 years or more are exposed well before.

For evidence, one need look no further than the 2015 breach at the Office of Personnel Management (OPM), of personnel records for 22 million U.S. government employees and family members. For spy agencies, theft of the security clearance records is uniquely painful – whoever gains access to the breached files will have an unparalleled ability to profile individuals in the intelligence community and subject them to identity theft.

OPM is just one instance in a long string of high-profile breaches, where hackers gain access to personal information, trade secrets, or classified government material. The focus of the discussion here, though, is on complementary trends in information technology, including the continuing effects of Moore's Law, the sociology of the information technology community, and changed sources and methods for signals intelligence. This article is about those risks of discovery and how the intelligence community must respond.

My views on this subject were formed during my experience as one of five members of President Obama's Review Group on Intelligence and Communications Technology in 2013. There is a crucial difference between learning about a wiretap on the German Chancellor from three decades ago and learning that a wiretap has targeted the Current German Chancellor, Angela Merkel, while she is still in office and able to object effectively. In government circles, this alertness to negative consequences is sometimes called "the front-page test," which describes how our actions will look if they appear on the front page of the newspaper. The front-page test becomes far more important to decision-makers when secrets become known sooner. Even if the secret operation is initially successful, the expected costs of disclosure become higher as the average time to disclosure decreases.

The greater relevance of the front-page test has direct and important implications for governance of secret intelligence operations. For good security reasons, intelligence agencies have historically been insular, relying on heavily vetted employees, with proven loyalty and discretion, and working in Secure Classified Facilities surrounded by physical and electronic barriers. This insularity, however, makes it harder for intelligence agencies to predict how diverse outside actors will view revelation of a secret program. As this article contends, the declining half-life of secrets is an important factual reason to bring greater transparency and more perspectives into the governance of sensitive signals intelligence activities. As of June 2015, the Obama administration had already taken a series of measures, consistent with the Review Group's recommendations, in that direction.[1] These changes, however, were difficult to accept within the intelligence community; understanding the declining half-life of secrets will help the community better assess what is possible and optimal for the less-secret future.

THE DECLINING HALF-LIFE OF SECRETS

The term "half-life" in physics indicates the time needed for a quantity to fall to half of its value as compared to its initial quantity. The term is most notably used for radioactive decay of atoms – how long it takes for half of the plutonium atoms, for instance, to decay into different elements or isotopes. For those trying to keep a secret, a leak is analogous to radioactive decay –

there is a potentially toxic effect when the secret leaves its previous location.

For our purposes, an important feature of the term "half-life" is that it the release is (at least largely) random. No one can predict in advance precisely which atom will decay, but the statistical average is nonetheless quite meaningful. Similarly for secrets, there may be no good way to estimate which secrets will get leaked at what time. An average leak within a few months, however, is more radioactive for the secret-holding agency than an average leak that takes much longer.

During the Cold War, the United States developed the basic classification system that exists today. Under Executive Order 13526, an executive agency must declassify its documents after 25 years unless an exception applies, with stricter rules if documents stay classified for 50 years or longer. These time frames are significant, showing a basic mind-set of keeping secrets for a time measured in decades.

Nonetheless, three factors drive the decline in the half-life of secrets: the continuing effects of Moore's Law – or the idea that computing power doubles every two years, the sociology of information technologists, and the different sources and methods for signals intelligence today compared with the Cold War. This article asks the reader to contemplate the implications if important secrets often get revealed in months or a few years.

THE CONTINUING EFFECTS OF MOORE'S LAW REDUCE SECRECY

The continuing improvement in computing is familiar to us all, but its implications for secrecy are less well understood. One implication is for the size of leaks. When Daniel Ellsberg leaked the Pentagon Papers in 1971, the magnitude seemed enormous, over 7,000 pages in 47 printed volumes. Snowden, by contrast, took between 50,000 and 200,000 documents, according to former NSA Director Keith Alexander.[2] Today a 64 gigabyte thumb drive costs less than $30, and holds over 4 million pages of text.[3] One full thumb drive is a gusher, not a leak. That is why one government expert quipped to the Review Group that "my goal is to have leaks get out only by printer."

The Internet makes it easy to disseminate these leaks. Ellsberg struggled to get the Pentagon Papers published. The lawyers for the New York Times initially recommended not publishing, although they eventually relented. Gatekeepers such as newspapers can be sued and are subject to persuasion by government that a leak should not be published, as occurred for the Times itself when it decided to delay the story about warrantless wiretaps from before the 2004 elections until December 2005.[4]

The gatekeepers, however, have far less power today to shut the gates. Wikileaks has shown that innumerable files can be posted to the Web without the assistance of the mainstream media. Reporters who received files from Snowden have, in some instances, decided not to print material due to concerns about harm to national security. But the ability of the government to rely on gatekeepers, to prevent publication, has declined sharply.

Other well-known trends of modern computing put secrets at further risk. The Internet of Things is based on a pervasive network of sensors. Big Data refers to the analytic ability to find patterns where none could previously be seen. Crowd sourcing means that far-flung individuals can coordinate their knowledge. Taken together, these trends can be applied to the activities of the intelligence agencies themselves. Spy satellites, for instance, can be followed from the

ground based on data from amateur astronomers around the globe. Drone strikes and the CIA's extraordinary rendition flights of a decade ago have similarly been discovered.

Intelligence agencies have long employed the mosaic theory, where multiple small bits of information about a target are brought together to form an accurate picture. Now, the ability to form the accurate picture has been democratized; given the smallest clue, reporters and the general public can often reconstruct an agency's activities.

THE SOCIOLOGICAL CHALLENGE TO NSA SECRECY

The NSA and other secret intelligence agencies face fundamental challenges in the sociology of those keeping their secrets. Other writers have mentioned this challenge, but the challenge to the NSA is central to the world-view of much of the information technology community.

A Foreign Affairs article from 2013 by science fiction writer Charles Stross emphasized the breakdown of lifetime employment, even for intelligence agencies.[5] He argued leaks would become more common by "nomadic contractor employees" who have almost no loyalty to their employers and thus are willing to spill secrets. ACLU technologist Chris Soghioian has shown that contractors spill secrets for a simpler reason – they often list their work experience, including even the names of classified programs, on LinkedIn as they search for the next job. These leaks by contractors were not intended to tip off outsiders; instead, the data leaks became more likely due to the contractors' having temporaryily worked on one project, needing to find the next project, and having less-complete immersion in any one agency's culture.

The likelihood of leaks by techies goes far beyond the shift from 30-year employees to contractors. There is a cultural and philosophical chasm between Silicon Valley and Washington, exemplified by the question of whether Snowden should be considered a traitor or a whistleblower. During my work on the Review Group, I spoke with numerous people in the intelligence community. Not a single one said that Snowden was a whistleblower. The level of anger toward him was palpable.

By contrast, a leader in a major Silicon Valley company said during the same period that more than 90 percent of employees there would say that Snowden was a whistleblower. The gap between zero and over 90 percent is a sociological chasm. It does not bode well for intelligence agencies that depend on cutting-edge information technologists.

The celebration of leakers has become an important theme in the culture of information technologists. Internet researcher danah boyd has written that, "leaking information is going to be the civil disobedience of our age."[6] Cyber-security guru Bruce Schneier agrees and offers two reasons.[7] First, physical protests are increasingly ineffective compared to online protests and releases of information. Second, the protests are specifically about secret courts, secret laws, and secret programs, so revealing the secret is the strongest response to power.

The approval of leaks fits with the techie opposition to secrecy. The well-known slogan that "information wants to be free" traces back to Stewart Brand, founder of the Whole Earth Catalog (which Steve Jobs once called "one of the bibles" of his generation). Chelsea (formerly Bradley) Manning quoted this phrase as a rationale for her leaks.[8] The open source movement exemplifies this philosophy: even lines of software code should not be kept secret.

For those not immersed in the culture of Silicon Valley, the world-view of EFF is one useful

example of the information technologist worldview. I am not affiliated with EFF, but have often worked with its activist technologists and lawyers. Among many other crusades, EFF supplied the lawyers to defend whistleblower Mark Klein, who revealed in 2006 that his employer AT&T had created a secret room in its San Francisco office to send bulk Internet communications to the government. EFF awarded its Pioneer Award in 2008 to Klein, calling him a hero. Snowden has similarly received a hero's welcome from technologists, as evidenced by his video appearance in 2014 at the South by Southwest conference.

The NSA and other secret agencies thus face a formidable problem: how to guard secrets when much of the information technology talent has anti-secret and libertarian inclinations. Federal agencies have long faced challenges in hiring top technology talent, for reasons including low pay and the need to pass background checks. But those challenges are more daunting in the wake of the Snowden leaks. The NSA can't stop hiring IT talent or impose a loyalty oath, screening out all those who sympathize with the widespread EFF-flavored views. That sort of ideological screening for government employment is likely illegal, and would cause an even deeper rift with the IT community. The sociology of information technology professionals thus poses a systematic threat to intelligence agency secrets.

THE CHANGING SOURCES AND METHODS FOR SIGNALS INTELLIGENCE

Signals intelligence during the Cold War used sources and methods that, in retrospect, we can see were relatively unlikely to lead to leaks. As Director of National Intelligence James Clapper has testified, much of the intelligence collection concerned separate communications systems – vanishingly few communications in the Warsaw Pact crossed over into Western telephone or other communications systems.[9] Much of the signals intelligence was done passively, such as by listening posts around the edges of the Soviet Union. Where surveillance was more active, it often was done with relatively trustworthy partners, notably AT&T and the other national monopolies. In addition, the sociology of the Cold War was conducive to secrets. The individuals who cooperated with the NSA were highly unlikely to wish to aid the Communists by revealing sources and methods. Where Soviet spies existed, the leaks were to the other side, and not to the general public. Ellsberg's leak of the Pentagon Papers was so notable precisely because it revealed the end of the consensus among insiders that secrets must remain secret from the public. By contrast, three changes in the methodology and targets of signals intelligence today make leaks far more likely.

First, signals intelligence agencies no longer have the Cold War luxury of focusing on geographically separate communications systems. For counter-terrorism efforts since September 11, a major priority is to identify potential or actual terrorists, who hide in the vast sea of other communications. Potential terrorists, as well as communications users in war zones such as Iraq and Afghanistan, use the same mobile phones, laptops, and other consumer devices as citizens of the United States and EU member states. Civilians and intelligence targets alike use the same operating systems, encryption protocols, apps, and other software. Because of this, exploits developed for the battlefield or to spot terrorists work against civilian systems. This convergence of citizen and target communications gives an important new rationale to leak – the public has a right to know about programs that spy on ordinary citizens and political dissidents. Members of Congress have a similar desire to uncover the truth, as shown by the repeated questions to the administration about whether the PATRIOT Act Section 215 telephone meta-data program gathered information on the calls of Senators and Representatives.

Second, the shift from passive listening posts to active intrusion is an additional reason why leaks are becoming more likely. Listening posts are generally outside of the area under surveillance, and the act of listening does not provide clues to the targets about what is occurring. By contrast, intrusion carries with it the risk of intrusion detection. Intrusion detection is now a pervasive part of system security. Thus, penetration by an intelligence agency or others has to cope with sophisticated defensive measures that bring attacks to light. Once an intrusion is detected, system owners are getting much better at attribution. As former NSA and Homeland Security official Stewart Baker has written: "It looks as though one aspect of computer technology is going to favor the defense. More and more data is being collected about network activities, making it harder for attackers to completely cover their tracks."[10] In short, attacks will be detected sooner rather than later, and cybersecurity professionals are getting better at tracing the attackers. That is terrifying news for any intelligence agency that expects its actions to remain secret for the traditional time span of 25 years or more.

Third, the nature of those holding communications has similarly changed. The Cold War was fought in an era of monopoly communications companies such as AT&T and government-run PTT's (post, telephone, telegraph) in other countries. These large companies had longstanding relationships with the government. They employed cadres of individuals with security clearances, and often government experience, to carry out law enforcement and national security wiretaps.

Today, communications are spread across a large and growing number of companies that lack the same structures for trusted sharing with the government. When Facebook paid $1 billion for Instagram in 2012, the latter company had 30 million users but only 13 employees.[11] In a world where competitive new social network and other communications providers arise constantly, many communications of interest to a signals intelligence agency take place within companies with no track record of keeping intelligence agency secrets.

The NSA and other signals intelligence agencies face a dilemma when reaching out for communications while trying to keep their own efforts secret. Today, the NSA targets terrorists and others, most of whom happen to use the same devices, software, and networks as ordinary citizens. If the NSA seeks to gain information without permission from the device manufacturers or system owners, then it must overcome the firewalls and intrusion detection systems of experts at cybersecurity defense. Such intrusions may succeed for a while, but they will rarely remain secret through years and generations of software upgrades. On the other hand, if the NSA seeks information with the permission of a system owner, it might be targeting the equivalent of Instagram, or companies with no infrastructure for keeping national security secrets. Or it might need to target the West Coast giants that dominate the free webmail market, but those companies are tightening their security to prove to global purchasers that they are not in bed with the NSA. And those companies employ technologists inclined to leak about questionable programs. The NSA thus faces serious risks of disclosure when it employs modern sources and methods, either with or without the permission of system owners.

THE FRONT-PAGE TEST

The argument thus far has been descriptive: the half-life of secrets is declining sharply. Modern computing means that leaks can be at scale and transmitted globally, while pervasive sensors and Big Data analytics outside of government can spot many once-secret agency activities. The

sociology of IT professionals means that secrets at odds with the EFF sensibility may well get exposed. And the sources and methods of intruding into civilian communications are far more at risk of exposure than during the Cold War. With all of these factors combined, it is extremely risky for the NSA or other signals intelligence agencies to assume that their activities will remain secret for anything like the traditional 25 years or more when secrets are officially declassified.

How should intelligence agencies respond to these changed facts? A likely first response is denial – surely there are counter-measures to these unpleasant changes! Some such counter-measures undoubtedly make sense, such as the recommendations by the Review Group on how to provide better cybersecurity for classified government computer systems. But the possibility of leaks, intentional and not, remains significant among the five million persons with U.S. government security clearances, and 1.5 million with Top Secret clearances, as reinforced by the loss of the security clearance information by OPM.

A second way to deny the declining half-life of secrets is to identify types of intelligence that can still remain secret. Targeted and covert operations may fit this bill better than signals intelligence collected from the masses. Even for covert ops, however, modern data streams pose difficult challenges. For instance, it is becoming more difficult to create and maintain a cover identity. Along with the growth of identity fraud has come a sophisticated industry devoted to spotting fake identities. And it is harder to create undercover agents when an operative without a Facebook history looks highly suspicious, but convincingly faking years of social media posts is also very difficult. Just as personal privacy is more difficult to protect in many circumstances, so too are covert personalities or operations. Comprehensive denial of exposure looks increasingly infeasible.

So if important secrets thus come to light, some of them quickly, then we must plan for the possibility of disclosure. In practice this means a more systematic use of the front-page test for activities of intelligence agencies. Walter Pincus of the Washington Post, however, has disagreed. In response to the Review Group's support for greater use of the front-page test, he wrote: "In some 40 years of covering intelligence, I have never heard of such a rule, nor have several former senior intelligence officials with whom I spoke."[12] Pincus wrote that, "The public's opinion shouldn't matter, because espionage, clandestine intercepts of intelligence and covert acts carried out by the United States and other governments are often, by their nature, dirty and mostly illegal operations where they are carried out." Pincus' views echo the famous quote by Jack Nicholson in the movie "A Few Good Men," when he told Tom Cruise: "You can't handle the truth." In the same speech, Nicholson added: "And my existence, while grotesque and incomprehensible to you, saves lives. You don't want the truth because deep down in places you don't talk about at parties you want me on that wall."

While we need defenders on that wall, the public's opinion will, and should indeed, matter. After all, that's the meaning of democracy, as well as the reality of having allies in democracies in Europe and elsewhere. In purely realist terms, moreover, the expected value of the harms from a secret operation rises sharply if the secrets become known soon. Jack Goldsmith, Harvard professor and former senior Bush administration lawyer, has largely agreed in an essay entitled "A Partial Defense of the Front-Page Rule."[13] He writes that, "Secret intelligence actions – especially the ones that would most likely engender outrage, surprise, debate, or legal controversy—are increasingly difficult to keep secret." Goldsmith recommends that intelligence actions related to the U.S. homeland or U.S. persons thus have a concrete and comprehensive plan to respond to unauthorized public disclosure in a convincing way. The NSA and other intelligence agencies will need to become more nimble in responding to press requests, but

a 24/7 news cycle and the cultural gap between press openness and IC secrecy mean that the agencies will usually be playing from behind.

CONCLUSION: GOVERNING INTELLIGENCE WHEN SECRETS BECOME KNOWN

Decisions about governance should follow from an accurate understanding of the world. Although the Snowden leaks remind us all that leaks are possible, systematic trends in computing, the sociology of the IT community, and the sources and methods of signals intelligence together make intelligence programs in the future far more difficult to conceal than most have realized, even apart from deliberate hacks on targets such as the OPM.

This factual change leads to numerous possible policy changes. The 46 recommendations and 300 pages of the Review Group's report discuss these changes in depth. One organizing theme is that governance of intelligence agencies and their programs should incorporate the multiple goals of U.S. policy. For instance, we recommended and the President has established a new process for White House review of sensitive intelligence collection. The review will assess national security as well as other goals such as relations with allies, economic and other foreign policy effects, and protection of privacy and civil liberties. Similarly, the President has created a new process to assess surveillance of foreign leaders, and our recommendation specifically included assessing the negative effects if the leader became aware of the U.S. collection.

More broadly, in an era when secrets may become public in the near term, intelligence agencies such as the NSA will need to communicate and engage differently with other policy makers and the general public. Agencies have long been reluctant to provide transparency for fear of follow-up questions and assistance to those applying the mosaic theory to the agency's activities. But the failure to explain – to say it in ways that are persuasive on the front page – has greater costs now. The world responds to what it learns about the current activities of intelligence agencies. Ignoring those responses will be bad for the intelligence agencies and for the many goals of our nation and its allies.

ENDNOTES

1 Clark, Richard A. and Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein and Peter Swire. 2013. "Liberty and Security in a Changing World." *Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies.* Dec. 12. <http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf>.

2 Hosenball, Mark. 2013. "NSA Chief: Snowden Leaked Up To 200,000 Documents." *Huffington Post*. Nov. 14. <http://www.huffingtonpost.com/2013/11/14/nsa-snowden-documents_n_4276708.html>.

3 Lexis Nexis. 2007. "Discovery Services Fact Sheet: How Many Pages in a Gigabyte." *Lexis Nexis.* <http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf>.

4 Lichtblau, Eric. 2008. "The Education of a 9/11 Reporter." *Slate*. Mar. 26. <http://www.slate.com/articles/news_and_politics/politics/2008/03/the_education_of_a_911_reporter.single.html>.

5 Stross, Charles. 2013. "Spy Kids." *Foreign Policy*. Aug. 29. <http://www.foreignpolicy.com/articles/2013/08/28/spy_kids_nsa_surveillance_next_generation>.

6 boyd, danah. 2013. "Whistleblowing Is the New Civil Disobedience: Why Edward Snowden Matters." *danah boyd | apophenia*. July 19. <http://www.zephoria.org/thoughts/archives/2013/07/19/edward-snowden-whistleblower.html>.

7 Schneier, Bruce. 2013. "Government Secrecy and the Generation Gap." *Schneier on Security*. Sept. 9. <https://www.schneier.com/blog/archives/2013/09/government_secr_1.html>.

8 Poulsen, Kevin and Kim Zetter. 2010. "'I Can't Believe What I'm Confessing to You': The Wikileaks Chats." *WIRED*. June 10. <http://www.wired.com/2010/06/wikileaks-chat/>.

9 Clapper, James R. 2013. "Potential Changes to the Foreign Intelligence Surveillance Act: Open Hearing Before the H.P. Select Comm. on Intelligence." *113 Congress*. Oct. 29.

10 Baker, Stewart. 2012. "Cybersecurity and Attribution: Good News at Last?" *Skating on Stilts*. Oct. 7. <http://www.skatingonstilts.com/skating-on-stilts/2012/10/my-entry.html>.

11 Teitelman, Robert. 2012. "Facebook, Instagram, and the Disciplines of Mergers and Acquisitions," *Huffington Post.* Apr. 11. <http://www.huffingtonpost.com/robert-teitelman/facebook-instagram_b_1418168.html>.

12 Pincus, Waler. 2013. "'Front-Page Rule' is unprecedented in U.S. intelligence community." *Washington Post*. Dec. 25. <http://www.washingtonpost.com/world/national-security/front-page-rule-is-unprecedented-in-us-intelligence-community/2013/12/25/2ddb25f8-6c0a-11e3-b405-7e360f7e9fd2_story.html>.

13 Goldsmith, Jack. 2014. "A Partial Defense of the Front-Page Rule." *The Hoover Institution.* Jan. 29. <http://www.advancingafreesociety.org/the-briefing/a-partial-defense-of-the-front-page-rule/>.

This Page Left Intentionally Blank