The NSA and Snowden: Securing the All-Seeing Eye

How good security at the NSA could have stopped him

Bob Toxen

Edward Snowden, while an NSA (National Security Agency) contractor at Booz Allen Hamilton in Hawaii, copied up to 1.7 million top-secret and above documents, smuggling copies on a thumb drive out of the secure facility in which he worked, and later released many to the press.² This has altered the relationship of the U.S. government with the American people, as well as with other countries. This article examines the computer security aspects of how the NSA could have prevented this, perhaps the most damaging breach of secrets in U.S. history.¹⁹ The accompanying sidebar looks at the Constitutional, legal, and moral issues.

According to Presidential Executive Order 13526, “‘Top Secret’ shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.”²⁴ There are clearance levels above top secret, such as SCI (sensitive compartmented information), SAP (special access programs), and CNWDI (critical nuclear weapon design information).⁹ The British equivalent to *top secret* is *most secret*.

WHAT DID SNOWDEN DO?

Snowden was a computer system administrator. Guarding against rogue sysadmins is more difficult than guarding against users, but it can be done. Note that the NSA has an almost infinite budget and resources, and thus could have been following good security practices all along. In the words of White House cybersecurity adviser Richard Clarke, “If you spend more on coffee than on IT security, you will be hacked. What’s more, you deserve to be hacked.”²⁰

National Public Radio’s “All Things Considered” last December 17 stated that the stolen documents were on Microsoft’s SharePoint document-management system. Of the 1.7 million documents likely copied, Snowden shared up to 200,000 documents with reporters; the NSA did not dispute this.^{2,19} Rick Ledgett, head of the NSA’s task force assessing the “damage” done by Snowden, claimed “system administrators... have passwords that give them the ability to go around those... security measures, and that’s what Snowden did.”¹⁹

That the NSA’s Ledgett claims to be unaware of the past 30 years of computer security techniques and technology for preventing a system administrator from stealing data is puzzling.^{10,15,29} This is discussed later in the “Orange Book and Two-person Authorization” section. The NSA no longer uses SharePoint for this purpose, which begs the question, why did the NSA abandon secure Orange Book compliance and other good security practices for computer systems that handle classified data?

In an interview with CBS’s “60 Minutes,” on December 15, General Keith B. Alexander, director of the NSA, admitted that part of Snowden’s job was to transfer large amounts of classified data between NSA computer systems.¹⁹ Snowden then copied files to a USB memory stick and concealed it on his person to smuggle vast amounts of data out of the NSA.^{11,26} A simple one-minute scan on the way out by a handheld metal detector—“wandering,” as used by the TSA (Transportation Security Administration) and at courthouses—would have found any flash memory device.

RINGS OF SECURITY

Let's digress briefly to discuss the important concept of *rings of security*, my term for the industry-standard but less obvious term *security in depth*. This means having multiple concentric rings of security so that if attackers get through the first or outermost ring that they encounter, then, hopefully, the second or third or fourth ring will stop them; no one security measure is 100 percent effective. These rings mostly are about authentication and are unrelated to what a user is allowed to do once authenticated. Consider how rings of security might apply to an ordinary network; this ordinary level of security is insufficient where very high security is needed such as the NSA, banks, systems handling large numbers of Social Security or credit-card numbers, etc.

Suppose we want to have a network in which sysadmins can SSH (Secure Shell) into a server from home. In the first ring the firewall might allow SSH access only from a short list of IP addresses of the sysadmins' home systems. Thus, instead of being able to attack from any of a billion systems on the Internet someone would have to launch her attack from one of, perhaps, a dozen system administrators' home networks, a vastly reduced vulnerability profile. Modern TCP/IP implementations, used by SSH, are very immune to IP spoofing. When combined with end-to-end encryption, person-in-the-middle attacks are virtually eliminated.

The second ring might allow SSH authentication only via public/private keys on these home systems. Prohibiting SSH from accepting passwords prevents password-guessing risks and thus access from unauthorized systems. The third ring would monitor log files for attacks and block those IPs, preferably automatically. The fourth ring would be a strong passphrase on that SSH private key. A fifth ring could require sysadmins' home systems (and, of course, all systems at the office) to lock the screen after a few minutes of inactivity.

STOPPING SNOWDEN

There are a number of security methods the NSA could have used which would have stopped Snowden. Many of these have been in use for a decade or more, yet the NSA did not use them.

ISLANDS OF SECURITY

The obvious place to start in this case is with preventing sysadmins or others from getting into unauthorized systems. The islands-of-security concept is a safeguard in case someone manages to penetrate the network. In a high-security organization, different segments, even different systems, should be treated as islands of security that do not trust each other or the network in the vast ocean of systems. This means different systems should have different root passwords, different user passwords, and different SSH passphrases, and almost all traffic between systems should be encrypted. Systems should have encrypted file systems and encrypted backups.

PHYSICAL SECURITY

Each island of security should be physically protected against attack. This certainly would include the systems and peripherals and the network carrying any unencrypted confidential data. Even large commercial collocation facilities have steel cages around some systems and video cameras watching these areas. The PCI (payment card industry) security standard requires such protection for large credit-card processors. High-security operations should install video cameras and keep the recordings for a long time.

One simple safeguard is to put two high-security locks on each cage, each lock needing a different key possessed by a different person. Thus, two people must be present when the hardware is accessed. Similarly, networking cables could be secured (e.g., inside of steel pipe), or the data encrypted before sending it around the local- or wide-area network. There is no reported indication that Snowden took advantage of any lack of physical security, although it is critical for protection.

PREVENT UNAUTHORIZED COPYING

The ability to plug in a USB memory stick or insert a blank DVD for writing should be disabled. Most DVD burners and USB jacks should be removed as well. Cameras, recorders, mobile phones, and any other unauthorized storage devices should be forbidden and guarded against. Metal detectors at doors would detect violators. RF (radio frequency) emissions should be monitored, and Faraday cages could be incorporated to block RF emissions. None of these techniques is expensive.

TWO-FACTOR AUTHENTICATION

Even Snowden's top-secret clearance wasn't sufficient to allow him access to some of the documents he stole. The NSA admitted that Snowden used the higher-than-top-secret clearances of the user accounts of some top NSA officials. This was possible because he had created these accounts or used his sysadmin privileges to modify the accounts to access even more highly classified documents remotely using NSAnet, the NSA's classified intranet.¹³ Snowden's access to accounts with higher security clearance than his violated the long-accepted security policy that the system should prevent anyone from accessing data with a higher clearance than the user's. It would have been a trivial matter for the computer to prevent this and instead require the services of a system administrator with that higher clearance level to adjust those accounts as needed.

This also violated the concept of two-factor authentication. Authentication is the ability of a computer (or security guard or even a store clerk) to determine if you really are who you claim to be. Typically, an authentication method consists of what you *know* (password or PIN), what you *have* (credit card or RFID-equipped badge issued to employees and consultants or USB dongle), or what you *are* (your signature or fingerprint or retina scan or your picture on a hard-to-forge document such as a driver's license, employee badge, or passport). Each of these is called a *factor*. None of these methods is expensive, and all are effective. While fingerprints can be faked with some effort, this is more difficult with modern high-quality fingerprint readers, which are available commercially.

Many organizations use the very popular two-factor authentication to grant access to computers or facilities or money, requiring, for example, that one does not get access without providing a password or an RFID-equipped badge *and* a fingerprint. Three-factor authentication would be even better.

Had the NSA required good two-factor authentication, such as a fingerprint and password compared against central databases to which Snowden didn't have administrative access, it would have prevented him from impersonating others to use their accounts—which is how he obtained documents above his security clearance. Collecting these factors for the databases would be done by two different sets of people, neither being the set that manages classified documents as Snowden did. This separation of authority is critical for good security as it requires multiple people to effect a compromise.

Even if the person managing users' passwords went rogue, she would not have access to the

fingerprint database. The password manager could be prevented from seeing the user entering his password by having the user enter a separate inner room via a one-person mantrap to which the person managing password changes does not have access. That room would have a virtual keyboard on a physically hardened touchscreen, making rogue use of a keystroke logger difficult. Lack of space here does not allow discussion of deeper exploits such as spoofing fingerprints, guarding against keyloggers, TEMPEST (the NSA's own set of security standards for radio frequency leakage of information), social engineering, etc.

Social engineering is where an attacker tricks someone into revealing information that he should not reveal. Those emails falsely claiming to be from your bank asking you to click on a link and provide your password or offering to share stolen money with you are examples. Snowden used social engineering to obtain the password of at least one NSA employee who subsequently resigned; the subject has been addressed extensively in other papers and books. Good recurrent education and strict policy forbidding sharing one's passwords, badge, dongle, etc. under any circumstance might have prevented this part of Snowden's breach.

ORANGE BOOK AND TWO-PERSON AUTHORIZATION

Someone is less likely to do something dishonest if someone else is watching. This is why many stores have at least two people working and why armored car services use two people. It also is why you see "Two signatures required for amounts over \$5,000" at the bottom of some checks.

The NSA created the Orange Book specification for Trusted Computer System Evaluation Criteria 30 years ago, requiring the federal government and contractors to use it for computers handling data with multiple levels of security classification. This author enhanced one Orange Book-compliant Unix system to have additional security capabilities. Such a computer would prevent, say, a user with only secret clearance from viewing a top-secret document. One also could create different "compartments" in which to keep separate sets of documents. Only someone allowed access to a particular named compartment could access documents in that compartment, even if that person otherwise had sufficient security clearance.

This high-security clearance is known as "compartmentalized security" (a.k.a., "need to know"). An important aspect of protecting a body of secrets is that very few people should have access to more than a small portion of them. A person working with one critical compartment should be barred from accessing other critical compartments. Those who know many of the secrets, such as General Alexander, get constant Secret Service protection.

One compartment might be "spying on Americans' phone records without a valid warrant." Another might be "listening to Americans' domestic phone conversations and reading email without a valid warrant."^{3,12,17,22} A third might be "hacking the phones of leaders of allied countries." As Snowden should not have been involved in any of those projects and thus should lack sufficient clearance, he would not have been able to access those programs' documents or even know that they existed. In reality, however, the NSA allowed one person, Snowden, unfettered, unmonitored access to 1.7 million documents.

Also important is the Orange Book concept of not trusting any one system administrator. Instead, a role-1 sysadmin queues system changes, such as new accounts or changes to an existing accounts. A second person, in role 2, cannot initiate such requests but must approve the queued requests before they can take effect. An Orange Book OS also prevents use of a login simulator by displaying

a special symbol when soliciting a password that no other program can display. Snowden may have used a login simulator.

How expensive might this two-person authorization have been? In 2013 the NSA had approximately 40,000 employees and perhaps 40,000 contractors, including 1,000 sysadmins.^{8,25} Adding another 1,000 system administrators to watch the first set would have increased the payroll by a trivial 1 percent.

Given this, is the NSA going to adopt two-person authorization and the Orange Book policy that it created? No, the NSA is going to fire 90 percent of its system administrators to limit human access and put most of the servers in the NSA's own cloud.¹ A cloud is just another name for a set of computers remotely accessible over a network and typically managed by others, usually a vendor (a.k.a., contractor). Maybe it will hire Booz Allen, Snowden's former employer, to manage this cloud.

LOG EVENTS AND MONITOR

The NSA should monitor how many documents each person accesses and at what rate, and then detect and limit this. It is astonishing, both with the NSA's breach and similar huge thefts of data such as Target's late-2013 loss of data for 40 million credit cards (including mine), that nobody noticed and did anything. Decent real-time monitoring and automated response to events would have detected both events early on and could have prevented most of each breach.

The open source Logcheck and Logwatch programs will generate alerts of abnormal events in near real-time, and the Fail2Ban program will lock out the attacker. All are free and easily can be customized to detect excessive quantities of downloads of documents. There are many comparable commercial applications, and the NSA certainly has the budget to create its own.

NO INTERNET ACCESS OR HOMEWORK WHATSOEVER

Obvious, this policy is to prevent classified data from leaving a secure building. For after-hours problems, a sysadmin either must drive to the office or be on-site at all times. One former CIA director nearly was fired for taking classified data home to work on, violating a strict policy against it. (He was not stealing the data; he just wanted to work at home.) Snowden took classified material home and worked on it with a hood covering him and the computer so that his girlfriend could not see it.¹⁹ Clearly, then, he could have photographed the screen.

PREVENT REMOVABLE MEDIA FROM LEAVING THE BUILDING

Recall the rings of security. One ring would prevent removable media from leaving the building. Every gas station owner has figured this out, attaching a large object to each restroom key. The NSA could put each thumb drive inside a large steel box, or it could replace the standard USB connectors and those of the computers with custom-designed connectors that are hard to duplicate.

CREATIVELY USE ENCRYPTION

Consider that one of Snowden's jobs was copying large amounts of classified data from one computer to a thumb drive and then connecting that thumb drive to another computer and downloading the data. He likely secreted the thumb drive on his person after downloading the data he wanted and took it home. This theft could have been prevented rather easily with the use of public-key encryption.³³ In public-key encryption there are two related keys: a public key and a secret key,

also called a private key. If the original “clear text” is encrypted with the public key, then it can be decrypted only with the secret key, not with the public key used to encrypt the data.

The NSA should have had a public/secret key pair created for each sysadmin who needed to transfer data and a separate account on each computer for each sysadmin to transfer this data. The person generating this encrypted data on the source computer (e.g., Snowden) would have to provide the ID of the public key of a different sysadmin—say, Julia—to the custom program allowed to write to the USB thumb drive; the software would not allow his own public key to be used. The set of sysadmins allowed to do transfers of data would have no members in common with the set of sysadmins on the source and destination computers with root access. In other words, a “Data Transfer System Administrator” such as Snowden would not have root or physical access to computers, and sysadmins having root or physical access would be prohibited from transferring data between systems. This separation of responsibilities is critical. Only that custom program, not sysadmins, would be allowed to write to the thumb drive. That computer would encrypt the data with Julia’s public key and write that encrypted data to the thumb drive.

Snowden then would download the encrypted data to the destination computer via the thumb drive using a custom program on the destination computer (with that program having sole access to the USB drive) after he had logged into his account. That program would prompt Snowden for the account in which to transfer that encrypted data (e.g., Julia’s), and then move the encrypted file to her account. Julia would log in to the destination computer and provide the passphrase that unlocks her encrypted secret key and her fingerprint or RFID-equipped badge to that custom program, which then would decrypt that data into Julia’s account. After that, she could move the data to the final location on the destination computer. The implementation is trivial.

Needless to say, the sysadmins tasked with this data transfer would not have the root (administrative) access to these computers that would allow them to get around this custom program’s restrictions, and these computers would be running modern versions of Orange Book-compliant operating systems that would require two system administrators for privileged access in any case. Furthermore, Snowden would not have Julia’s fingerprint or passphrase or, if used, her badge for authentication. The open source GPG (GNU Privacy Guard) stores private keys on disk or elsewhere in an encrypted form that can be decrypted only by providing a passphrase or other authentication.¹⁵

Thus, no sysadmin acting alone could decrypt data that he or she encrypted to a thumb drive. This would have prevented Snowden’s theft by thumb drive. These custom programs (which would run on the source and destination computers) could be written in a day or two using the open source GPG encryption program by a substantial percentage of those reading this article. Thus, even if a USB thumb drive was smuggled out of a secure NSA facility, it would have no value.

Similarly, there could be an additional ring of file-level encryption for highly classified files with separate public/secret key pairs. Only those users entitled to read these documents (and not the sysadmins tasked with copying files) would have the secret keys to decrypt them. Those using the destination system (after legitimate copying by Snowden and Julia) would be able to decrypt the files. The system administrator, however, would never have seen the decrypted documents even by reading the raw disk. By itself, this simple precaution would have prevented the wholesale theft of many documents by Snowden. Combined with the use of public-key encryption for transferring data between systems, Snowden would have had to defeat two extremely challenging rings of security

to steal data. Using encrypted file systems or whole-disk encryption on all computers handling classified data would offer an additional ring of security.

PLAN FOR BREAK-IN TO MINIMIZE DAMAGE

The NSA's Ledgett acknowledges, "We also learned for the first time that part of the damage assessment considered the possibility that Snowden could have left a bug or virus behind on the NSA's system[s], like a time bomb."¹⁹ The agency should have planned for a possible break-in to minimize the harm and quickly and reliably assess the damage. For example, it could be prepared to compare a system's current state with a trusted backup taken before the break-in. This comparison could be run on a different and trusted system.²⁹ The use of islands of security and not putting all of the NSA's eggs in one basket would have minimized the damage. It could have been running a file-system integrity checker all along to detect tampering with files.

PERIODIC SECURITY AUDITS

Security is an ongoing process. An outside security audit performed quarterly or annually would have found the NSA's problems and, perhaps, fixed them in time to stop Snowden. Such an audit is quite common and considered good practice. This is similar to the outside financial audit of large companies required by... the U.S. government. The audit report should be reviewed by the highest levels of management to avoid lower levels simply ignoring inconvenient findings.

SUMMARY

The NSA seemingly had become lax in utilizing even the most important, simple, and cheap good computer security practices with predictable consequences, even though it has virtually unlimited resources and access—if it wants it—to the best computer security experts in the country.

Most of the good security practices covered here were discussed in the author's *Real World Linux Security*, first published in 2000.²⁹ The most important of these security practices also were discussed in this author's article, "The Seven Deadly Sins of Linux Security," published in the May/June 2007 issue of *ACM Queue*.

I am honored that there are autographed copies of my book in the NSA's headquarters. The vast majority of NSA employees and contractors are eminently talented, law-abiding, dedicated patriots. It is unfortunate that a tiny percentage no doubt ignored warnings that these security problems desperately needed fixing to avoid a serious breach.

Constitutionality

Another critical aspect of the NSA's spying on all Americans is the constitutionality and morality, which is what Snowden was trying to draw attention to—and succeeded in a big way. The Constitution's Fourth Amendment says this:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Why did the framers of the Constitution care, and why should we care? In short, because when enforced by honest and competent judges, the Fourth Amendment prevents serious abuse by government officials against innocent people, including intrusion into their private matters. In colonial America, Britain's King George empowered officials to conduct mass searches of houses, persons, their effects, etc. without a warrant or probable cause, despite the English Court's *Saman's Case* of 1603, which recognized the right of the homeowner to defend his house against unlawful entry even by the king's agents in the absence of a specific warrant based on probable cause.^{6,31} This is the meaning behind "Every man's house is his castle." (One of the most powerful expressions of that maxim came from William Pitt speaking to Parliament in 1763, "The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail... but the King of England cannot enter—all his force dares not cross the threshold of the ruined tenement.")

It was confirmed in England in 1705 in *Entick v. Carrington*. The English court decided that a general warrant that caused the raiding of many homes—including Entick's, which the king's men broke into and whose locked desks and boxes were broken into as well, with the seizure of many documents unrelated to what was being searched for—was against English law. The court held that the warrant used against Entick was too general, not based on probable cause, and allowed the seizing of unrelated material; and, further, no record was made of what was seized. Take note that the court case was initiated by Entick suing the crown.^{16,31} Is not one's computer and phone the modern equivalent of a locked desk?

On December 28, 2013, U.S. Judge William H. Pauley III held that an American may not file suit against the NSA for spying on Americans. Specifically, he dismissed a lawsuit by the ACLU (American Civil Liberties Union), saying, "The ACLU would never have learned about the section 215 order authorizing collection of telephone metadata related to its telephone numbers but for the unauthorized disclosures of Edward Snowden."^{7,34} Section 215 of the Patriot Act requires that this spying on Americans be kept secret forever. Electronics certainly qualify as personal belongings, which is how the Oxford English Dictionary defines effects. One's effects are protected by the Fourth Amendment.

Pauley's ruling says that an American may not challenge the constitutionality of a government action because the American found out about it only through the illegal action of another. That ruling sounds more like the former Soviet Union to the author. It also is contrary to more than 200 years of U.S. Constitutional law precedent which holds that a person, regardless of citizenship, always is entitled to all Constitutional rights and always may challenge a violation. The only government defense is that no violation took place.

A 1969 U.S. court ruling found that "the [Fourth] Amendment was in large part a reaction to the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence [i.e., the American Revolution]. In the scheme of the Amendment, therefore, the requirement that 'no Warrants shall issue, but upon probable cause' plays a crucial part."^{4,31} Many more similar U.S. court rulings can be found with little effort. In short, a reasonable search requires probable cause, meaning a good reason to believe that someone possesses something illegal or evidence of a crime.

According to the judicial branch of the U.S. government, "Whether a particular type of search is

considered reasonable in the eyes of the law is determined by balancing two important interests. On one side of the scale is the intrusion on an individual's Fourth Amendment rights. On the other side of the scale are legitimate government interests, such as public safety."³⁰ "Yet, the parameters of the Fourth Amendment do not cease in the realm of searching electronic devices."¹⁸

President Obama's own independent PCLOB (Privacy and Civil Liberties Oversight Board) says that the NSA's phone-spying program is illegal and should end, *The Washington Post* revealed. "We have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation," the 238-page report says.

PCLOB's report also says that the NSA phone data program cannot be grounded in section 215 of The Patriot Act, which "requires that records sought by the government [e.g., phone numbers] be relevant to an authorized investigation."²⁸ Seizing all phone records of all Americans "just in case" clearly is not reasonable by any possible interpretation of the Constitution.

On December 16, 2013, U.S. Federal Judge Richard J. Leon ruled that bulk collection of telephone metadata of American telephone companies likely violates the U.S. Constitution. The judge wrote, "I cannot imagine a more 'indiscriminate' and 'arbitrary' invasion than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval... Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment." Leon said the government "does not cite a single instance in which... the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the government..."²¹

Recently my friend Josh asked me about the NSA's spying on Americans, adding, "Well, if it helps to catch terrorists, I don't mind them spying on me." I pointed out that in sworn testimony before Congress, General Keith B. Alexander, director of the NSA, admitted that not a single American life has been saved by the NSA's deliberate spying on 300 million Americans. I asked him what he thought about some NSA analyst listening in on a romantic conversation with his wife. He did not seem so happy about it now.

Josh has a young daughter, so I asked, "What if in a few years as a 16-year-old, your daughter phones you saying, 'Daddy, I'm at a friend's. Could you come get me? I've been drinking and I'm not safe to drive. I'm really sorry.'" How would Josh like it if the NSA listened to that conversation and provided the local police with his daughter's location using the phone's GPS and a transcript of that private phone conversation, and the police then arrested his daughter for underage drinking? Josh got real unhappy at this point. Are you trying to keep your sexual orientation or interests private? How about your religious beliefs or even whom you voted for in the Presidential election? What about that stock tip or patent idea? Is it the government's business to know whom you are telephoning?

Yes, the NSA really is listening to your domestic phone calls and reading your e-mail in addition to obtaining your private information on the people you telephone.^{3,12,17,22} Reuters reported on August 5, 2013, that the DEA (Drug Enforcement Administration) admitted to covering up the use of information illegally obtained from the NSA and falsifying the source of evidence. This included information obtained by the NSA from intelligence intercepts, wiretaps, informants, and a massive database of telephone records, all without benefit of a proper warrant or probable cause. The DEA

then gave this information to authorities across the nation to help them launch criminal investigations of Americans.²⁷ Clearly this is exactly what the Fourth Amendment was intended to prevent. Is it the government's place to be doing this?

Judge Andrew P. Napolitano, the youngest person ever to serve on the New Jersey Superior Court, called President Obama's promised NSA reforms, announced January 17, 2014, a presidential placebo.^{23,32} The EFF (Electronic Frontier Foundation) rated the President's reforms 3.5 out of 12.⁵ (The EFF is a nonprofit organization dedicated to fighting for people's rights in the electronic world and is, perhaps, the most active organization to fight in the courts and elsewhere against the NSA's spying on Americans.) Sen. Rand Paul (R-Ky.) argued that Obama's suggested changes will amount to "the same unconstitutional program with a new configuration."¹⁴ Many of these actions by the NSA were started under the second Bush Administration following 9/11. Is the NSA's spying on all Americans an unconstitutional and illegal violation of the Constitution's Fourth Amendment? Given the 400 years of history that we have examined, this author can see only one conclusion.

REMEMBRANCE

The author mourns the death of Stan Kelly-Bootle, friend and mentor for 35 years, computer pioneer who earned the world's first post graduate degree in computer science (from Cambridge), author of nine books on computers and over a hundred articles and columns including his hilarious long-time Queue Curmudgeon column. Stan also was a famous singer and songwriter, collaborating with many singers including Peggy Seeger, Pete Seeger, Judy Collins, The Dubliners, and occasionally performing on the BBC from 1958 to 2011.

Stan Kelly-Bootle, 1929-04/16/2014.

REFERENCES

1. Allen, J. 2013. NSA to cut system administrators by 90 percent to limit data access. Reuters. August 9; <http://www.reuters.com/article/2013/08/09/us-usa-security-nsa-leaks-idUSBRE97801020130809>.
2. Block, M. 2013. Snowden's document leaks shocked the NSA, and more may be on the way. National Public Radio. December 17; <http://www.npr.org/templates/story/story.php?storyId=252006951>.
3. Brosnahan, J., West, T. 2006. Brief of Amicus Curiae Mark Klein. May 4; <https://www.eff.org/files/filenode/att/kleinamicus.pdf>.
4. *Chimel v. California*, 395 U.S. 752, 761 (1969).
5. Cohn, C., Higgins, P. 2014. Rating Obama's NSA reform plan: EFF scorecard explained. Electronic Frontier Foundation, January 17; <https://www.eff.org/deeplinks/2014/01/rating-obamas-nsa-reform-plan-eff-scorecard-explained>.
6. Coke's Reports 91a, 77 Eng. Rep. 194 (K.B. 1604).
7. Davidson, A. 2013. Judge Pauley to the N.S.A.: Go Big. *The New Yorker*. December 28; <http://www.newyorker.com/online/blogs/closeread/2013/12/judge-pauley-to-the-nsa-go-big.html>.

8. Davidson, J. 2013. NSA to cut 90 percent of systems administrators. *Washington Post*. August 13; <http://www.washingtonpost.com/blogs/federal-eye/wp/2013/08/13/nsa-to-cut-90-percent-of-systems-administrators/>.
9. Defense Logistics Agency. Critical nuclear weapon design information access certificate; <http://www.dla.mil/dss/forms/fillables/DL1710.pdf>.
10. Department of Defense Trusted Computer System Evaluation Criteria, a.k.a., Orange Book 1985; <http://csrc.nist.gov/publications/history/dod85.pdf>.
11. Dilanian, K. 2013. Officials: Edward Snowden took NSA secrets on thumb drive. *Los Angeles Times*. June 13; <http://articles.latimes.com/2013/jun/13/news/la-pn-snowden-nsa-secrets-thumb-drive-20130613>.
12. Electronic Frontier Foundation (eff.org). NSA spying video, includes comments from many well-known respected people and reminders of past violations; http://www.youtube.com/watch?v=aGmiw_rrNxk.
13. Esposito, R. 2013. Snowden impersonated NSA officials, sources say. NBC News. August 28; http://investigations.nbcnews.com/_news/2013/08/28/20234171-snowden-impersonated-nsa-officials-sources-say?lite.
14. Everett, B., Min Kim, S. 2014. Lawmakers praise, pan President Obama's NSA plan. Politico. January 17; <http://www.politico.com/story/2014/01/rand-paul-response-nsa-speech-102319.html>.
15. GNU Privacy Guard; <http://www.gnupg.org>.
16. Howell's State Trials 1029, 95 Eng. 807 (1705).
17. Klein, M., Bamford, J. 2009. *Wiring Up the Big Brother Machine...and Fighting It*. Booksurge Publishing.
18. Legal Information Institute, Cornell University Law School. Fourth Amendment: an overview; http://www.law.cornell.edu/wex/fourth_amendment.
19. Miller, J. 2013. CBS News "60 Minutes." December 15; <http://www.cbsnews.com/news/nsa-speaks-out-on-snowden-spying/>.
20. Lemos, R. 2002. Security guru: let's secure the Net. ZDnet; <http://www.zdnet.com/news/security-guru-lets-secure-the-net/120859>.
21. Mears, B., Perez, E. 2013. Judge: NSA domestic phone data-mining unconstitutional. CNN. December 17; <http://www.cnn.com/2013/12/16/justice/nsa-surveillance-court-ruling/>.
22. Nakashima, E. 2007. A story of surveillance. *Washington Post*. November 7; <http://www.washingtonpost.com/wp-dyn/content/article/2007/11/07/AR2007110700006.html>.
23. Napolitano, A. P. 2014. A presidential placebo – Obama's massive NSA spying program still alive and well. Fox News. January 23; <http://www.foxnews.com/opinion/2014/01/23/presidential-placebo-obama-massive-nsa-spying-program-still-alive-and-well/>.
24. Presidential Executive Order 13526 12/29/2009; <http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information>.
25. Rosenbach, M. 2013. Prism exposed: data surveillance with global implications. Spiegel Online International. June 10: 2; <http://www.spiegel.de/international/world/prism-leak-inside-the-controversial-us-data-surveillance-program-a-904761.html>.
26. Schwartz, M. 2013. Thumb drive security: Snowden 1, NSA 0. *InformationWeek*. June 14; <http://www.informationweek.com/infrastructure/storage/thumb-drive-security-snowden-1-nsa-0/d/d-id/1110380>.

27. Shiffman, J., Cooke, K. 2013. Exclusive: U.S. directs agents to cover up program used to investigate Americans. Reuters. August 05; <http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805>.
28. Smith, C. 2014. BGR. January 23; <http://news.yahoo.com/watchdog-says-nsa-phone-spying-program-illegal-end-130014396.html>.
29. Toxen, B. 2002. *Real-world Linux Security: Intrusion Detection, Prevention, and Recovery*. 2nd Edition. Prentice Hall.
30. U. S. Courts. What does the Fourth Amendment mean?; <http://www.uscourts.gov/educational-resources/get-involved/constitution-activities/fourth-amendment/fourth-amendment-mean.aspx>.
31. U.S. Government Printing Office. Fourth Amendment; <http://beta.congress.gov/content/conan/pdf/GPO-CONAN-2013-10-5.pdf>.
- Washington Post. 2014. Transcript of President Obama's Jan. 17 speech on NSA reforms; http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.
33. Wikipedia. Public-key cryptography; http://en.wikipedia.org/wiki/Public-key_cryptography
34. Wikipedia. Edward Snowden; http://en.wikipedia.org/wiki/Edward_Snowden#NSA_rulings_in_federal_court.

LOVE IT, HATE IT? LET US KNOW

feedback@queue.acm.org

BOB TOXEN (bob@VerySecureLinux.com) is chief technical officer at Horizon Network Security, which specializes in Linux and network security. He was one of the developers of Berkeley Unix.

© COPYRIGHT HELD BY THE AUTHOR. PUBLICATION RIGHTS LICENSED TO ACM. \$15.00