Health Technol. (2017) 7:501–517
DOI 10.1007/s12553-017-0205-3

ORIGINAL PAPER

The end of privacy for the populace, the person of interest and the persecuted

Diane Roark[1]

Received: 11 November 2016 / Accepted: 18 June 2017 / Published online: 17 July 2017

Abstract Erosion of US and foreign citizens' privacy has resulted from the escalating use of electronic devices; creation of gargantuan commercial and government/intelligence databases; government access to business data; and the motivation and ever more sophisticated ability to mine and unaccountably use such information. After suffering the terrorist attacks of September 11, 2001, the US government led the way in globally collecting and exploiting personal data. This ultimately required revisions to existing US law, as well as altered legal interpretations of constitutional protections for civil liberties. The overwhelming focus of US communications and electronic storage policy has been on offensive intelligence operations; collection has been enhanced partly by undermining cyber defense for companies and citizens. As with other business sectors, US medical information now is vulnerable to both criminal cyber-attack and government access. This article is authored by a former US intelligence community and national security professional with highly specialized proficiencies and experience at some of the top levels of intelligence oversight – where technical, operational, analytic, in- ter-agency, legislative, regulatory, legal and budget activities converge. Using unclassified and public sources, the author summarizes the types and breadth of US domestic collection and its distribution, the degree to which individuals' privacy may be impinged, abuse of these powers, and effects on governance. Resulting US ability to spot and forestall pending domestic terror attacks - the rationale used to justify surveillance without end - is evaluated.

This article is part of the Topical Collection on *Privacy and Security of Medical Information*

✉ Diane Roark
gardenofeden@wvi.com

[1] Stayton, OR, USA

Keywords Privacy · Data protection · Surveillance · Whistleblower · National Security Agency · NSA · US civil liberties · Terror attacks

1 Introduction: surveilling the populace

These days, an individual can be fairly certain to retain privacy in prudent and trusted face-to-face conversations; in secured papers that are either handwritten or typed on a computer that is never connected to the Internet; and perhaps in cash transactions patterned well below $10,000 each. This assumes no search, either overt or surreptitious, of one's home or business. All else is alarmingly vulnerable to collection by third parties, and to amassing and automated scanning of our individual files if desired.

Exposure to commercial tracking and government surveillance will continue to grow rapidly along with advancing technology such as enhanced data mining, new personal identification techniques and artificial intelligence. This trend can be slowed or reversed only under exacting conditions. In the US, permissive laws such as the USA PATRIOT ACT and the FISA Amendments Act of 2008, plus regulations such as Executive Order (E.O.) 12333, would have to be revoked. Privacy law must be updated to the digital age. User-friendly, unbreakable encryption and other technology protections geared to ordinary individuals must be permitted, funded and developed. US federal court decisions eroding civil liberties protections must be reversed or overridden by new statutes. And effective, technologically sophisticated, independent, intrusive verification of intelligence agency conduct would have to exist. In the meantime, governmental control over citizens is escalating globally, with citizen freedoms and democratic control eroding to a point where reversal would be most difficult.

In many countries, as in the US, metastasizing government surveillance is excused in the name of safety from terrorism. Yet in the US, massive domestic espionage has impeded, rather than enhanced, the prevention of pending domestic attacks. Tiny droplets of clues are submerged in vast oceans of mass collection.

At considerable taxpayer expense, this surveillance data pads the personal dossiers of a US population of 319 million persons. Americans are at greater risk of consequent loss of freedom than are foreign persons upon whom the US collects, because the US government has no direct power over most foreign private citizens. However, their own governments often also are surveilling them.

The umbrella code word for US domestic surveillance was "STELLARWIND," [1] at least until Edward Snowden revealed that name and some of the programs falling under it, beginning in June 2013. The accumulated domestic surveillance records may provide information more quickly and fully *after* a domestic attack or after a tip from elsewhere on whom to investigate, when normal police work might dig up much of the same information. However, the rationale behind STELLARWIND has always been quite specific and different - to provide the very first alert and tipoff of a pending attack, and most especially about any "lone wolf" attacker unconnected to a terrorist organization. [2] In this, it persistently fails. Yet STELLARWIND is perpetuated and enhanced, while our collected private information is distributed ever more widely.

The US Government domestic surveillance programs pose an existential threat to both individual liberty and democracy. History appears to present no conclusion with more proof than the historian Lord Acton's summation that "power tends to corrupt, and absolute power corrupts absolutely," [3] or, as Edward Abbey similarly put it: "power is always dangerous…. power attracts the worst and corrupts the best…" [4].

Public defense of US domestic spy programs is replete with known lies, evasions and ruses, a red flag signaling the rot of corruption. Throughout all history, there has been no greater absolute knowledge and power over individuals than that inherent in the goliath bureaucratic state's ability to act on the information in these dossiers, should it so desire. Is that why the intelligence agencies are still collecting it?

2 Commercial collection of intelligence

Most US employers reserve the right to inspect employee workplace electronic trails. All customer activity is potentially subject to tracking by businesses seeking to profit from refining their ad placements, or from the sale of their contact lists, or from "mining" their customer "big data" that might be "anonymized" to greater or lesser extent.[1]

Many of the apps on one's smart phone collect data related to one's activities. As with a desktop computer, use of a cell phone is increasingly tracked so that targeted ads may be placed, with the added benefit that one's location might also be known by the same tracking.

The much ballyhooed promotion of the "Internet of Things" (IoT) sells often-insecure devices that are used to manage homes electronically. This demonstrably threatens one's remaining shreds of privacy. It also leaves Internet-connected thermostats, DVDs, alarms, baby monitors, electronic personal assistants, etc. subject to takeover for "botnet" attacks on third-party websites.[2] Eavesdropping on conversations within one's vehicle[3] (by exploiting installed two-way emergency communication services) and collection of vehicle operating history (advocated by insurance companies) are also possible. Vehicles increasingly dependent on sophisticated electronics are becoming vulnerable to remote electronic takeover, raising the possibility of secret sabotage.[4]

"Cloud" computing is also promoted as among the latest and greatest electronic innovations, with the data of individuals and businesses stored at specialized commercial electronic warehouses for a fee. It is reasoned that experts at these stores will be better able than private individuals to protect data from cyber-attack. This may be offset, however, by the fact that such a huge target is evident and enticing to malicious hackers,[5] and because the US government may

[1] Big data is a phrase used to describe the accumulation of a massive volume of structured and unstructured data. Data mining is referred to here, as the searching, analyzing and sifting through large amounts of data to find relationships, patterns, or any significant statistical correlations.

[2] Segal, Liron; "Mirai: The IoT Bot That Took Down Krebs and Launched a Tbps DDoS Attack on OVH," F5 Labs, October 7, 2016. https://f5.com/about-us/news/articles/mirai-the-iot-bot-that-took-down-krebs-and-launched-a-tbps-ddos-attack-on-ovh-21937 and "This botnet with 145,607 cameras/dvr (1-30Mbps per IP) is able to send >1.5Tbps DDoS. Type: tcp/ack, tcp/ack + psh, tcp/syn", Twitter - **Octave Klaba / Oles, CEO - OVh** https://twitter.com/olesovhcom/status/779297257199964160

[3] Fox-Brewster, Thomas; "Cartapping: How Feds Have Spied On Connected Cars For 15 Years," Forbes, Jan 15, 2017 https://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/#119d87c32ef8 AND Woodyard, Chris and O'Donnell, Jayne; "Your car may be invading your privacy," USA TODAY, March 24, 2013 (Updated 11:45 a.m. ET March 25, 2013) http://www.usatoday.com/story/money/cars/2013/03/24/car-spying-edr-data-privacy/1991751/#

[4] Associated Press; "Hackers hijack car computers and take the wheel: Security experts show modern vehicles potentially vulnerable to cyber attacks," CBS News, 13 Sep. 2013 http://www.cbc.ca/news/technology/hackers-hijack-car-computers-and-take-the-wheel-1.1322678

[5] Mearian, Lucas; "No, your data isn't secure in the cloud," Computerworld, August 13 2013 http://www.computerworld.com/article/2483552/cloud-security/no–your-data-isn-t-secure-in-the-cloud.html AND McMillan, Robert; "Got $500? You can buy a hacked U.S. military website," IDG News Service, January 21 2011 http://www.computerworld.com/article/2512560/government-it/got–500–you-can-buy-a-hacked-u-s–military-website.html

be able legally to seize or copy your data without a warrant if it is not in your home.

3 US intelligence collection

3.1 Business records

The US government has surveillance capabilities far beyond those of commercial Internet companies. Edward Snowden revealed that the government can, for instance, turn on a computer or cellphone microphone, or camera, in order to use the device against its owner. However, under the business records provision within the October 2001 USA PATRIOT Act,[6] as renewed in subsequent legislation, ***all*** US business records, and not just those of huge communications and technology companies, must, upon government demand, be turned over to the FBI; and businesses are not allowed to notify the customer that they have done so.

In July 2002, this author became aware that US business databases with sensitive personal information were being collected by the US National Security Agency (NSA). This was a very early date, only ten months after STELLARWIND[7] commenced on October 4, 2001, and while NSA's other domestic communications intercept programs were still ramping up. Given the priority accorded to the collection of such non-communications 'business' information, in the author's view it is likely that other non-communications business databases subsequently were acquired or searched. Whistleblower Russell Tice has said that NSA data-mined credit card and other financial records.[8] Credit card records can show the type of item or service purchased; where and when it was bought, and other information on one's debt and financial health.

Collection of business records can, and often is, being done without the issuance of a ***warrant,*** based on the US Constitution's Fourth Amendment requirement of "probable cause" – when facts and circumstances are sufficient that a prudent person would believe an individual has committed, is committing, or is about to commit a crime. Sometimes the warrantless collection is done *en masse* (by the National Security Agency or other agencies), and other times while targeting individuals or relatively few people (e.g. by NSA, or by the Federal Bureau of Investigation (FBI) using "National Security Letters"). Blanket or individualized domestic warrants are issued by the federal Executive-Branch Foreign Intelligence Surveillance Court (FISC); for years, a single, updated order from the FISC required a telephone company to give the NSA and the FBI all of its US telephone metadata, for instance.

3.2 Executive order 12333

US intelligence collection is also justified under allegedly independent "Commander-In-Chief" Presidential powers[9] that purportedly are not subject to US Congressional review. Such powers include the re-interpretation of requirements under Executive Order (E.O.) 12333 (United States intelligence activities).[10] Some consider E.O. 12333 a likely source of massive collection of US citizens' information, conducted under the guise of foreign collection, but far exceeding Section 702 activity discussed below. Others state that a ***never-revealed October 4, 2001 paper*** provides legal justification and authorization for post-9/11 surveillance that goes far beyond the E.O.[11] A highly redacted White House legal memo of 2004 claims that Congress has no oversight over these aforementioned "Commander-In-Chief" (Presidential) powers:

> *The President has inherent constitutional authority as Commander in Chief and sole organ for the nation in foreign affairs to conduct warrantless surveillance of enemy forces for intelligence purposes to detect and disrupt armed attacks on the United States. Congress does not have the power to restrict the President's exercise of this authority.*[12]

[6] 50 U.S. Code § 1861 - Access to certain business records for foreign intelligence and international terrorism investigations. Source: Legal Information Institute - Cornell University Law School, Ithaca, NY https://www.law.cornell.edu/uscode/text/50/1861 AND Isikoff, Michael [National Investigative Correspondent]; "FBI sharply increases use of Patriot Act provision to collect US citizens' records," NBC News, 11 June 2013 http://investigations.nbcnews.com/_news/2013/06/11/18887491-fbi-sharply-increases-use-of-patriot-act-provision-to-collect-us-citizens-records

[7] Isikoff, *supra*, [1]

[8] Kim Zetter; "NSA Whistleblower: Wiretaps were Combined with Credit Card Records on U.S. Citizens," Wired, 23 Jan. 2009, http://truth-out.org/archive/component/k2/item/82168:nsa-whistleblower-wiretaps-were-combined-with-credit-card-records-of-us-citizens

[9] "*Commander in Chief Powers*" [Article II Section 2 of the U.S. Constitution], Legal Information Institute, Cornell University - Law School, Ithaca, NY https://www.law.cornell.edu/wex/commander_in_chief_powers

[10] *Executive Order 12333*, December 4 1981 (46 FR 59941, 3 CFR, 1981 Comp., p. 200) https://www.archives.gov/federal-register/codification/executive-order/12333.html

[11] Cyrus Farivar; "The executive order that led to mass spying, as told by NSA alumni," arsTECHNICA, Aug. 27, 2014 https://arstechnica.com/tech-policy/2014/08/a-twisted-history-how-a-reagan-era-executive-order-led-to-mass-spying/2/ See also: Mark Jaycox; "A Primer on Executive Order 12333: The Mass Surveillance Starlet," Electronic Freedom Foundation, June 2, 2014. https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet AND John Napier Tye, "Meet Executive Order 12333: The Reagan rule that lets the NSA spy on Americans," Washington Post, July 18, 2014, https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html?utm_term=.17fed7230348 Alex Emmons; "Obama opens NSA's vast trove of warrantless data to entire intelligence community, just in time for Trump," The Intercept, Jan. 17, 2017 https://theintercept.com/2017/01/13/obama-opens-nsas-vast-trove-of-warrantless-data-to-entire-intelligence-community-just-in-time-for-trump/

[12] *Farivar, Ibid*

In response to a Freedom of Information Act lawsuit filed by the American Civil Liberties Union and others, NSA released a legal fact sheet in September 2014, stating, "NSA conducts the majority of its SIGINT activities solely pursuant to the authority provided by E.O. 12333."[13] Almost all attention has been focused on legislation such as the Foreign Intelligence Surveillance Act (FISA, including the FISC court it established), the USA PATRIOT Act, the FISA Amendments Act of 2008, and other laws and updates, but these may be of relatively minor importance, and may also be interpreted in light of alleged secret authorities under the E.O.

3.3 Section 702

Because Internet and telephone traffic travels over fiber optic lines at the speed of light, companies routinely minimize costs by taking advantage of differing levels of activity in various areas and time zones, for instance, dynamically shifting even purely domestic traffic to less congested or cheaper lines abroad. A "loophole" was built into Section 702 of the FISA Amendments Act of 2008, a section that ostensibly dealt with foreign intelligence collection. Section 702 was interpreted as allowing the NSA to receive, store, and search for mention of identified intelligence targets within these domestic messages, that were returning to the US after being routed abroad.

Without a warrant, and since 2008, NSA has searched both the metadata (email "To, From," etc.) and message content of such US messages for mention of previously identified targets. A FISC judge ruled in 2011 that search of such content required a warrant, and therefore, the program was discussed more openly in 2013 after Edward Snowden's revelations. The FISC appeared to believe the collection was sufficiently widespread to be considered bulk collection.[14] The NSA eventually admitted to the Court that analyst content searches had for years violated the requirement for a warrant. In late April 2017, NSA opted to quit searching content, and to destroy almost all the Internet traffic of this type that had accumulated in Agency databases. Metadata will continue to be searched, however.[15]

Interpretation of NSA's conduct and its motives for finally confessing and for destroying the databases has sometimes been quite skeptical.[16] Section 702 expires toward the end of 2017, or after the latest judicial order permitting it runs out, unless Congress renews it.

Collection on US persons from domestic fiber optic lines is allowed if it is believed that there is over a 50% chance that a message might include foreign persons. It is unclear how these odds are calculated, but under such a targeting rule, large amounts of domestic data might be scooped up and stored. Former NSA senior executive William Binney contends that AT&T substations throughout the nation, and not just at border landfalls, are collecting data, and therefore, those in the interior are collecting primarily domestic communications.

3.4 Cooperating governments abroad

Some suspect that cooperating foreign governments, notably the United Kingdom's Government Communications Headquarters (GCHQ), have collected US domestic communications routed abroad and have provided them to the US, to skirt US law. The Edward Snowden documents revealed that the GCHQ swept up even more communications than did the NSA. It has also been confirmed that the US provided UK domestic communications to GCHQ, skirting UK law.[17]

3.5 Additional US local and federal collection

The US government searches social media sites. It cooperates with local and state police to collect citizen photos for anticipated use of rapidly developing ***facial recognition***[18]

[13] Alex Abdo; "New Documents Shed Light on One of the NSA's Most Powerful Tools," ACLU, 29 Sept. 2014 https://www.aclu.org/blog/new-documents-shed-light-one-nsas-most-powerful-tools?redirect=blog/national-security/new-documents-shed-light-one-nsas-most-powerful-tools.

[14] B. Hanssen; "Why the NSA's Incidental Collection under Its Section 702 Upstream Internet Program May Well be Bulk Collection, Even If The Program Engages In Targeted Surveillance," https://medium.com/@BHanssen/why-the-nsas-incidental-collection-under-its-section-702-upstream-internet-program-may-well-be-a01817e161c

[15] Charlie Savage; "N > S > A > Halts Collection of Americans' Emails About Foreign Targets," New York Times, April 28, 2017. https://supporters.eff.org/civicrm/mailing/view?reset=1&id=2153

See also: EFFector No. 718, "What you need to know about "about" searches." https://supporters.eff.org/civicrm/mailing/view?reset=1&id=2153 AND Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, July 2,2014. https://www.pclob.gov/library/702-report.pdf

[16] John Solomon and Sara Carter; "Obama intel agency secretly conducted illegal searches on Americans for years," Circa, 24 May 2017 http://circa.com/politics/barack-obamas-team-secretly-disclosed-years-of-illegal-nsa-searches-spying-on-americans AND Bob Unruh; "Breakthrough in Fight over NSA Internet Spying," WND, 23 May 2017 http://www.wnd.com/2017/05/breakthrough-in-fight-over-nsa-internet-spying/ AND Jason Koebler; "This Is the Secret Court Order That Forced the NSA to delete the Data It Collected About You," Motherboard, 11 May 2017 https://motherboard.vice.com/en_us/article/this-is-the-secret-court-order-that-forced-the-nsa-to-delete-the-data-it-collected-about-you

[17] Karla Adam; "GCHQ-NSA Intelligence Sharing Unlawful," Washington Post, Feb. 6, 2017 https://www.washingtonpost.com/world/gchq-nsa-intelligence-sharing-unlawful/2015/02/06/193adda2-e66e-46fd-9759-b85d45ab022a_story.html?utm_term=.e4f3e37923f0

[18] "Local, State and Federal Law Enforcement Partnering to Create Massive Facial Recognition System," Tenth Amendment Center, http://tenthamendmentcenter.com/2016/10/31/local-state-and-federal-law-enforcement-partnering-to-create-massive-facial-recognition-system/ AND Volz, Dustin, "Rights groups request U.S. probe police use of facial recognition," Reuters, Oct. 18, 2016, http://www.reuters.com/article/us-usa-cyber-face-recognition-idUSKCN12I2AD SEE ALSO: Kevin Collier, "Vermont DMV Caught Using Illegal Facial Recognition Program: Local, state and federal law enforcement were allowed to search DMV photo database, documents show," Vocativ, 24 May 2017 http://www.vocativ.com/432762/vermont-dmv-facial-recognition-aclu/

technology. ***Fingerprint access*** to locked devices or areas is supplemented by ***Iris scans.*** Biometrics collected by the NSA[19] and others provide means to identify many more individuals than those associated with crime. If past practice is an indicator, federal and state police forces might employ such technologies without a warrant, pending discovery and successful legal challenge to the operations, steps that often take many years. Local ***public security cameras,*** subsidized by the federal government, are installed on many street corners and highways, with thousands of them in and near large cities, and a presence even in many smaller cities. Federal intelligence on citizens is shared with state and local police for criminal cases, not just to counter terrorism.

Police patrol cars with ***license plate readers*** can catalog the ownership and location of every car they meet. Automotive license plates in the parking lots at US gun shows have been scanned by local police at the request of federal agents [5] . ***Toll stations*** collect automotive license plate numbers and ***smart-pass identities*** [6]. Airplanes, helicopters, and drones ***impersonate cell towers*** and collect on everyone within a wide area. Until recently revealed, cell tower impersonations, like a multitude of other activities, were a secret carefully kept away from the US public and US courts. And for good reason – a Baltimore court and a Maryland appeals court[20] ruled the use of the Stingray technology in question to be illegal if conducted without a warrant based on probable cause, which is required to track a cell phone location.

The movie "Minority Report"[21] and the CBS television series "Person of Interest"[22] no longer seem like extreme departures from reality, as confirmed by the 2017 CBS reality television series "Hunted."[23]

Highly intrusive surveillance techniques, often originally developed and justified for domestic anti-terror purposes, have inappropriately been crossing over to regular criminal law enforcement applications. US local and state law enforcement entities have gained access to parts of some federal databases.[24] Safety from criminals or madmen, and not just from terrorist attack, is increasingly portrayed as more important than privacy, and thus more important than freedom. Fifteen years on, the 'national security state' is transitioning to a 'police state.'[25]

Reuters revealed in August 2013[26] that an arm of the US Department of Justice (DoJ), the Drug Enforcement Administration (DEA), routinely cooperates with two dozen partner agencies, including its sibling FBI, NSA and the Internal Revenue Service (IRS), to compile a one-billion record database. The database includes such things as wiretaps and many telephone records. These records are being used for criminal as well as national security purposes, to apprehend narco-terrorists, organized crime and drug gangs. About 10,000 law enforcement officers at that time had access to the database, and without any specific warrants. The origins of resulting investigations are hidden from defendants, courts, and sometimes even prosecutors, through "parallel construction" of a falsified evidentiary trail, thereby violating defendant due process rights[27] under the US Constitution.

In *Clapper v. Amnesty International*, the only case on NSA surveillance that reached the United States Supreme Court to date, the DoJ went so far as to pre-screen and approve the successful, but false, argument of an unknowing Solicitor General. US Solicitor General Donald Verilli assured the Court that a better case on wiretapping without a warrant inevitably would become available, because in lower courts the government would have to reveal such surveillance; thus, there would then be certain knowledge that a defendant had been surveilled under the NSA domestic program. However, DoJ had not been revealing this, and at that time, had no intention of doing so.[28]

[19] Biometric data is now a "standard NSA [tool]." Dana Priest; "NSA growth fueled by need to target terrorists," Washington Post, 21 July 2013 https://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html?utm_term=.0ff66958d34a

[20] Newman, Lily Hay; "How Baltimore Became America's Laboratory for Spy Tech," Wired, 4 September, 2016 https://www.wired.com/2016/09/baltimore-became-americas-testbed-surveillance-tech/ AND Justin Fenton, "Maryland appellate court: warrant required for 'stingray' phone tracking," The Baltimore Sun, March 31, 2016, http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-stingray-court-decision-20160331-story.html

[21] "*Minority Report,*" Steven Spielberg - Director, Gary Goldman and Ronald Shusett - Executive Producers, Scott Frank and Jon Cohen - Screenplay, twentieth Century Fox Film Corporation & Dreamworks SKG, Hollywood, CA, USA 2002

[22] "*Person of Interest,*" Created by Jonathan Nolan, Starring: Jim Caviezel, Michael Emerson, Kevin Chapman and Taraji Henson, Columbia Broadcasting System (CBS) Television Network, New York City, New York, USA (2011–2016)

[23] "Hunted", Created by Sean Travis, Brian Catalina & Laura Fuest - Executive Producers, Lock and Key Productions, Columbia Broadcasting System (CBS) & Endemol Shine North America, Los Angels, CA, 2017

[24] Law Enforcement Information Sharing, ISE Information Sharing Environment, https://www.ise.gov/law-enforcement-information-sharing AND Elinson, Zusha, FBI Lends Local Police a Hand," Wall Street Journal, Oct. 26,2015, http://www.wsj.com/articles/fbi-lends-local-police-a-hand-1445902822

[25] Radley Balko; "Surprise! NSA data will soon routinely be used for domestic policing that has nothing to do with terrorism," Washington Post, 10 March 2016 https://www.washingtonpost.com/news/the-watch/wp/2016/03/10/surprise-nsa-data-will-soon-routinely-be-used-for-domestic-policing-that-has-nothing-to-do-with-terrorism/

[26] Jeff Shiffman and Kristina Cooke; "Exclusive: U.S. directs agents to cover up program used to investigate Americans," Reuters, 5 August 2013 http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805

[27] The Fifth and Fourteenth amendments to the Constitution guarantee due process of law. "Procedural" due process includes, inter alia, protection from unconstitutional search and seizure, such as NSA collection without a warrant. A court may partially, or fully, exclude evidence under the exclusionary rule, which is designed to protect *Fourth Amendment* rights against unreasonable searches and seizures by law enforcement personnel. Prosecutorial misrepresentation of evidence may also impede an effective defense.

[28] Verilli insisted to the US Dept. of Justice (DoJ) that there was no legal basis to withhold the surveillance information, and the Justice Department eventually notified several defendants that their communications had been collected by NSA without a warrant. Savage, Charlie; "Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence," The New York Times, 26 October 2013 http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html

4 Government collection of unclassified records

A vast trove of data from all levels of government and other sources has been merged with the huge amount of classified information collected by intelligence agencies. Apart from the business records collected by NSA, the FBI, NCTC and US Postal Service are also primary hubs acquiring and combining such repositories. In general, the FBI now sweeps up information

> "*…from open or public source materials; federal, state or local government databases or pervasive information sharing programs; and private companies and then amasses it in huge data bases where it is mined for a multitude of purposes.*" [29]

Some of this may be transferred to the National Counterterrorism Center (NCTC).

4.1 National Counterterrorism Center

Compiling of classified terror tips from agencies with unclassified records of US residents took a great leap forward in March 2012. The database dragnet was extended to include enormous caches of unclassified federal agency information. This was in response to President Obama's demand that the "terrorist watch list" be overhauled after the "underwear bomber," Umar Farouk Abdulmutallab, in 2009 nearly brought down an airplane flying to Detroit on Christmas Day.[30]

As with the Fort Hood attacker, Major Nidal Hassan, U.S. authorities had been warned about Abdulmutallab. However, the US National Counterterrorism Center (NCTC) at the Central Intelligence Agency had failed to pursue the lead by querying databases. In addition, the plot was prepared in Africa, where Abdulmutallab's travel originated, and not in the US. Nonetheless, the response was to focus on getting still more domestic information to address the "lone wolf" threat. Further draconian measures targeting the US population were adopted.

In a journalistic coup of December 2012, reporter Julia Angwin[31] received, through Freedom of Information Act requests and government whistleblowers, documented and undisputed evidence that since March 2012, all US government agencies – not just intelligence agencies – can be forced to turn over their databases on US persons to the NCTC. This overturned provisions in prior privacy law.[32] NCTC henceforth was to serve as the central repository for all information that might possibly facilitate efforts to counter domestic or international terrorism. Its website lead proclaims "**….***We lead and integrate the national counterterrorism (CT) effort by fusing foreign and domestic CT information.*"[33]

John Brennan, then assigned to the White House as President Obama's chief counterterrorism advisor, who later became the Director of Central Intelligence, presided over a March 2012 meeting on the possible expansion of NCTC's powers. Within a week, Attorney General Eric Holder signed into effect a government dragnet sweeping up US persons' federal records. It eliminated prior privacy protections, permitted analysts to search the entire collected database for suspicious patterns of behavior, allowed NCTC retention of information for five years (or permanently if a person is deemed suspect), and also permitted US citizen databases to be given to foreign governments.[34]

Angwin relates that this decision was considered "*a breathtaking sea change in the Government's relations with its citizens*".[35] Every US federal department and agency was required to negotiate terms under which it would hand over huge databases full of information to the NCTC. By searching records acquired in the normal course of business with citizens, the government was expanding surveillance of residents much farther than the classified intelligence programs that were in place at the time, including those that had already grossly exceeded previously permissible police and intelligence activities. Every US citizen is now considered a potential suspect, Angwin related. Further, NCTC already had a poor reputation for adhering to privacy restrictions on transferred data.

These data sets would not normally be sought or considered particularly relevant until after a "probable cause" warrant was issued - and even then, only as they related to a specific case and circumstances. Now, however, they are

[29] ACLU, "Unleashed and Unaccountable: The FBI' Unchecked Abuse of Authority," September 2013, p. 19 (emphasis added) https://www.aclu.org/feature/unleashed-and-unaccountable

[30] Julia Angwin; "U.S. Terrorism Agency to Tap a Vast Database of Citizens," Wall Street Journal, Dec. 12, 2012 https://www.wsj.com/articles/SB10001424127887324478304578171623040640006?mg=id-wsj
The discussion below draws on this lengthy article. Angwin is presently with "ProPublica" [https://www.propublica.org/site/author/julia_angwin]

[31] *Ibid*

[32] Recognizing, even then, the substantial threat to privacy, the pre-digital Privacy Act of 1974 forbade agency sharing of data for purposes incompatible with the reasons for its collection. However, agencies were allowed to exempt themselves from many requirements simply by placing notices in the voluminous Federal Register, which they are doing after they negotiate terms with NCTC. [Angwin, cited above, and an overview of the Privacy Act at https://www.justice.gov/opcl/privacy-act-1974]

[33] The National Counterterrorism Center, Office of the Director of National Intelligence, Washington, DC. https://www.dni.gov/index.php/nctc-home [Emphasis added.]

[34] The reference to foreign governments at minimum infers to the UK's GCHQ, and perhaps also to other English-speaking "Five Eyes" intelligence services. It may also apply to Israel; transfer of data on US citizens to Israel was documented by Edward Snowden as revealed in Glenn Greenwald, Laura Poitras and Ewen MacAskill, "NSA shares raw intelligence including Americans' data with Israel," The Guardian, 11 Sept. 2013 https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents

[35] Emphasis not in the original

"reasonably believed" to include "terrorist information," just as the FISC had ruled concerning the entire nation's telephone and email communications.

The massive volume of records is deemed vital to the still-unsuccessful attempt to find *predictive patterns* of domestic terrorist behavior by combing through "big data." And, very "big" data it is indeed; so much so that NCTC had already been choking on prior federal data transfers.[36] The amount and wide-ranging content of federal agency information gives pause. The sheer range of information under federal agency custody extends from such things as lists of casino employees to examples such as motor vehicle and professional licenses, mortgage applications and federal tax records.

4.2 US postal service collection

One can currently avoid communications surveillance from hackers or businesses by using "snail mail." However, this will not foil the US government. After anthrax packets were mailed in 2001, the USPO supplemented its longstanding selective (but growing) "mail cover" program[37] with mass photography of the front and back of all letters, collecting the addressee, return address, postmark date and place, postage and insurance information. In essence this is postal metadata (although email has far more metadata fields). This Mail Isolation and Tracking System operates at over 200 locations,[38] an average of four per state. In 2012, the system photographed 160 billion pieces of mail. These photography requirements probably contributed to the USPO policy of initially sending all mail to often-distant central collection points, rather than immediately to its destination in a town perhaps two miles away. USPO packages also are now electronically entered into a system and tracked, similar to systems for package delivery by private companies.

The letter tracking was kept highly secret until information from it was cited in a 2013 report regarding letters containing the toxin ricin, that were sent to President Obama and New York Mayor Michael Bloomberg. All admit that it is a sweeping program, but the USPO defends itself by saying it is kept at separate sites and is not all collected into a single massive USPO database; this does not rule out the possibility that these feed into databases at the National Counterterrorism Center. The USPO is a quasi-federal entity, part government and part commercial.

In an apparent attempt to improve its competitiveness with commercial companies and email, the USPO has also just begun notifying some customers that a new "Informed Delivery" capability is being rolled out, to notify customers by email when they can expect a letter-sized delivery; this probably uses photographic information from the Mail Isolation and Tracking System, because detailed black and white images of prospective deliveries will be sent.[39]

If the sender is certain that the intended recipient is at the delivery address, to improve privacy somewhat, he could opt to avoid including a return address on the letter or using a credit card when mailing. The possibility that the mail will be opened and contents viewed cannot be ruled out if the government might be interested in activities of the sender or recipient.

5 Medical privacy

Medical records also might be construed as falling under US courts' "third party" doctrine,[40] under which one's records are more protected at one's home than at a business where you are a customer. In addition, many medical records are held by federal agencies that theoretically might even be required to transfer their data to the National Counterterrorism Center (NCTC), administered under the Director of National Intelligence.

US active duty military and veterans, whose health records are kept at military hospitals and veterans facilities, would appear most at risk of intelligence or police access to their records. The US Department of Homeland Security indicated years ago that it is wary of veterans who might have Post-Traumatic Stress Disorder. The Ft. Hood attack might have strengthened this view, and another factor could be this population segment's training in the use of weapons.

[36] Angwin, *supra* note (xxix) [Five months after agencies were told in January 2010 to send all their terrorist leads and tips to the NCTC following the "underwear bomber" attempt, and thus even before the March 2012 White House decision, NCTC had been flooded with huge backlogs. Two months after NCTC had previously received a database from the Department of Homeland Security (DHS), it still had not been fully uploaded. DHS had also provided information on foreign exchange students and their hosts, and details on visa applications. In addition, after the 2012 policy decision, DHS would move to transfer the Advanced Passenger Information System (APIS) with information on every airline passenger entering the US, as well as two other data sets - on non-citizen visitors to the US, and on people seeking refugee asylum. An APIS fact sheet is at: https://www.cbp.gov/sites/default/files/documents/apis_factsheet_3.pdf]

[37] For problems found in the Phase I investigation of the mail cover program involving law enforcement and national security requests, see Audit Report – Postal Inspection Service Mail Covers Program (Report Number HR-AR-14-001), Office of The Inspector General – USPS, Washington, DC, 28 May 2014 https://www.uspsoig.gov/sites/default/files/document-library-files/2015/hr-ar-14-001.pdf

[38] Nixon, Ron; "Postal Service Confirms Photographing All U.S. Mail," New York Times, Aug. 2, 2013 http://www.nytimes.com/2013/08/03/us/postal-service-confirms-photographing-all-us-mail.html, AND "U.S. Postal Service Logging All Mail for Law Enforcement," New York Times, July 3, 2013. http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html

[39] "Seeing What's In The Mail, Has Never Been More Convenient," USPS, See: https://informeddelivery.usps.com/box/pages/intro/start.action

[40] For a critique of the doctrine and a discussion of medical records, see Michael Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third Party Doctrine*, Brennan Center for Justice, June 29, 2015. Medical privacy is discussed at pp. 58–60. Also See Greg Nojeim, "Why the Third Party Records Doctrine Should be Revisited," American Bar Association. A contrary view is adjacent. http://www.americanbar.org/groups/public_services/law_national_security/patriot_debates2/the_book_online/ch4/ch4_ess10.html

The US government also provides Medicaid health assistance for lower income families, Medicare for the elderly, and insurance under the Affordable Care Act. All are administered by government agencies that must maintain extensive health and even financial records within large electronic databases.

Medical records are normally accorded significantly less public or private access than most other papers stored outside the home. Third Party doctrine may provide legal rights to the US government, however. According to US HIPAA[41] privacy forms, health providers are required to respond to court orders, court-issued warrants, subpoenas, and even administrative requests. The last could indicate that at the US federal level, only a National Security Letter (NSL) issued by the FBI, without a warrant, may be required, or even less. HIPAA-compliant[42] privacy forms vary, but now include a national security exemption to privacy rights and, in the author's recent experience, an additional and explicit intelligence exception – "*national security or intelligence considerations.*" A "*consideration*" is far removed from the "*probable cause*" of criminality needed for a legal warrant.

Most medical forms do not point out, however, that patients can refuse to sign off on portions of HIPAA, and thus avoid legally ceding some of their privacy rights. One can accept the normal business waivers for insurance companies, etc., but take action such as crossing out national security and intelligence access and writing "refused" plus your initials on the side margin. It might also be well to note in a prominent place that the form was partially rejected.

A major medical privacy issue is the determined US government push toward Electronic Medical Records, initially through federal monetary incentives, and then by penalizing laggards via reduced Medicare payments. An ultimate goal has been to centralize electronic records in some way, perhaps at the state level or directly at the federal agency level. President George W. Bush first advocated electronic records, but moves in this direction occurred under President Barack Obama's economic stimulus program and the Affordable Care Act. Large medical databases, however, are a magnet to criminal identity thieves, provide easier access to the government, and should be avoided when possible.

There have also been many documented and growing concerns about the security and privacy risks of electronic media in general. Information conducive to identity theft is always an issue, and medical records contain a great deal of personal information, including US Social Security Number, date of birth and medical history, that are highly prized by criminal cyber thieves. Patients are also concerned about theft of, or even widespread access to, sensitive medical information, including details that many choose not to reveal outside of their immediate family members and caregivers. During hospitalization, over two or three duty shifts at the facility, many people may gain access to a patient's electronic record. Outside the hospital, at insurance companies and elsewhere, even more people have access.

Electronic data breaches have become remarkably common in the medical area, where, by US law, statistics are collected and reported for breaches involving more than 500 people. In 2015, an astounding 112 million medical records were reported to be involved in data breaches,[43] compared to a U.S. population of 319 million. Protected health information is very valuable on the black market. An estimate of the average cost of a lost or stolen health record is $154, but, for healthcare organizations that are involved, it is $363 on average.[44] The bulk of these breaches were at large insurance companies.

Since 2009, HIPAA has required encryption for (stored) data "at rest," as well as for data "in motion" (being sent over the Internet). Rules are consistent with those of the U.S. National Institute of Standards and Technology (NIST), using the Advanced Encryption Standard (AES) for encryption algorithms.[45]

However, the NSA papers provided to reporters by Edward Snowden and published in September 2013 confirm that commercial encryption has been weakened by "back doors" facilitated by the US and the United Kingdom. It was claimed specifically that encryption used to protect medical records was affected.[46] In the US, such backdoors were long suspected to have been implemented through NIST, which must solicit NSA advice and guidance when issuing encryption standards. However, there had remained debate as to whether AES was insecure.[47]

[41] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191 https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

[42] *Ibid*

[43] Munro, Dan; "Data Breaches In Healthcare Totaled Over 112 Million Records In 2015," Forbes, December 31, 2015. http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#796cc0487fd5

[44] Pennic, Fred; "Report: Hackers Caused 98% of Healthcare Data Breaches in 2015," Jan. 28, 2016, HIT, http://hitconsultant.net/2016/01/28/hackers-caused-98-of-healthcare-data-breaches/

[45] HIPAA Email Compliance: 6 Best Practices for Medical Data Security," Virtu Blog, V irtu Corporation, Jan. 8, 2015 https://www.virtu.com/blog/hipaa-email-compliance/

[46] Ball, James, et al., "Revealed: how US and UK spy agencies defeat internet privacy and security," The Guardian, September 6, 2013. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[47] See Bruce Schneier, who helped reporters with the NSA documents. "The NSA is Breaking Most Encryption on the Internet," Schneier on Security, https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html

Compare this with Schneier's 2012 commentary: "Can the NSA Break AES?" Schneier on Security, https://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html Other commentaries include:

Aron, Jacob and Marks, Paul, "How NSA weakens encryption to access internet traffic," 6 Sept. 2013, New Scientist, https://www.newscientist.com/article/dn24165-how-nsa-weakens-encryption-to-access-internet-traffic/ AND Bright, Peter, "Leaked documents say that the NSA has compromised encryption specs. It wasn't always this way," September 5, 2013. Ars Technica, http://arstechnica.com/security/2013/09/the-nsas-work-to-make-crypto-worse-and-better/

Without a back door, "unbreakable" code often is broken by exploiting sloppy security procedures, as well as poor encryption implementation in coding.

Back doors allowing access to governments seeking to facilitate their own intelligence collection can also be exploited by others who find them, including foreign governments, criminal rings and individual hackers. Once such encryption flaws were confirmed in 2013, the race to find and exploit them would have begun. It is unclear whether countermeasures were taken by medical companies.

6 Existing privacy protections

The US Executive Branch has largely misled, lied to, and hidden from, voters the amount and types of their data that NSA and others are collecting. It is only due to whistleblowers and consequent press revelations that the public has any idea of its enormity.

There is also a major campaign to remove these issues from political discourse and public consciousness. Although published Snowden information is freely available to terrorists and others abroad, the documents have mostly been scrubbed off easily available US websites. The issue has mostly disappeared from mainstream media and from national campaigns. Federal employees have been banned from referencing or commenting on published material like Snowden's, on grounds that the data still is classified, despite its worldwide distribution.[48]

6.1 Access to domestic intelligence collection within NSA

Supplementing this campaign, since 2006 US administrations have issued a constant drumbeat of assurances that *within NSA*, access to domestic data is severely limited. This was indeed the case initially, when the main concern was to avoid media leaks, because the activity so clearly violated prior legal guidelines that every NSA employee had annually reviewed and signed.

Obviously, however, it would be useless to collect the enormous and growing flood of domestic data described above if only a very small number of NSA analysts had access to it. This is certainly no longer the case, as indicated by NSA's own admission to the FISC, also discussed above, that from 2008 to 2017 it had been unable to prevent analysts from querying the content of Section 702 domestic email collection. NSA also formally conceded that some NSA employees had tracked spouses and romantic interests, but Edward Snowden also said that as a systems administrator, he, like many others, had easy access to databases with domestic content. The administration likes to focus on a mere 22-person cadre, who have played a mostly hazy role in supposedly strictly limiting access to databases storing domestic communications. However, the Snowden documents revealed that analysts merely select from options in a drop-down menu to justify access to a domestic target identity.

6.2 NSA data copied to the FBI and others

With the entire focus on the NSA, the US administration and Congress have carefully avoided the mention of privacy controls over data sharing with other intelligence and non-intelligence agencies, contractors, law enforcement, and allied nations, plus with NCTC as partially discussed above. Just before President Obama left office in January 2017, the charade ended, when Mr. Obama directed distribution of raw NSA database content throughout all 17 intelligence agencies, so that information about alleged Trump team ties to Russia would be widely distributed, and therefore safe from destruction and undeniable. Possible limits on this sharing have not been revealed.

There has been almost no known scrutiny of other agencies' policies for protecting the privacy of Americans caught up in the NSA dragnet, whether their individual operations were inspected regularly, and whether any of the protections were effective. There are many more recipients of finished reports, into which raw data was incorporated; however, US identities are supposed to be "masked" by removing names and other material that could identify them. In later years of the Obama administration, more "unmasking" occurred.

Initially, the NSA gave the FBI many "tips" to investigate.[49] Eventually, the FBI was streamed copies of the raw NSA domestic email database, and the FBI then undertook its own analysis; presumably, NSA continued to provide tips from telephone and other computer collection. The FISC warrants for mass collection revealed by Edward Snowden in 2013 show that it was the FBI requesting these warrants, as well as extension of the warrants. The FBI was the primary user of results from domestic collection, for investigations. The National Counterterrorism Center eventually got all of the NSA intake and/or reports, too, under lax terms, and

[48] For instance, during his public confirmation hearings a month after Edward Snowden started revealing domestic surveillance programs, former FBI Director James Comey refused to discuss the revealed programs on grounds that he was not familiar with current details, while opining that tools such as metadata collection could be useful against terrorism. Later he refused to comment because he claimed the programs were classified. See: Sari Horowitz; "Comey defends surveillance programs but says he's open to more transparency," Washington Post, 9 July 2013 https://www.washingtonpost.com/world/national-security/comey-defends-surveillance-programs-but-says-hes-open-to-more-transperancy/2013/07/09/167bf17e-e8a9-11e2-8f22-de4bd2a2bd39_story.html?utm_term=.a8424418727e

[49] Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr.; "Domestic Surveillance: The Program; Spy Agency Data After Sept. 11 Led F.B.I. To Dead Ends," New York Times, 17 Jan. 2006 http://www.nytimes.com/2006/01/17/us/front%20page/domestic-surveillance-the-program-spy-agency-data-after-sept.html

despite its poor reputation for enforcing privacy protections, as discussed above.

After the mass shooting by U.S. Army Major Nidal Hassan at Fort Hood in November 2009, it was revealed that the Department of Defense had ignored many signs of Hassan's radicalization, and that the FBI had not shared with the DoD any information on Hassan. Intelligence services belatedly pulled out their records of his emails to a prominent radical Islamist located in the Middle East. In response to a question from Senator Kohl, former FBI Director Mueller said the FBI aimed to improve analytical tools in the email databases, so as to enhance FBI capabilities. Those tools were described by Mueller as, "technological improvements relating to the capabilities of a data-base to *pull together past e-mails and future ones as they come in* so that it does not require an individualized search."[50] Clearly, this was regularly updated bulk email content from NSA, not just metadata.

Responding to a question for the record from Senator Grassley, the FBI said its Joint Terrorism Task Forces (JTTFs)[51] maintain "baseline" databases at the Secret or Unclassified level, as well as Top Secret Secure [Specially] Compartmented Information *(TS/SCI)* databases with information from NSA and CIA. The baseline databases are "typically" accessible to all trained and cleared JTTF employees, whether such employees are from the FBI, or Task Force Officers assigned from other jurisdictions, such as state and local governments. Use of the *TS/SCI* databases required "an articulable need for access." While JTTF personnel usually had those clearances, it could become a source of friction with state and local law enforcement, including those at the 70 State Fusion-Centers, where the FBI is often present.[52]

The failure to investigate Nidal Hassan adequately was said to be a training problem involving lack of knowledge about the *TS/SCI* databases, rather than an access problem. To resolve this deficiency, the FBI, which had *over 4000* people at the JTTFs, sent 3732 of them to Quantico, Virginia for database training.[53]

With an influx of money and growing demands that it prevent terrorist attacks, the FBI's budget request for FY 2012 swelled to over $8 billion, and its emphasis changed dramatically. In 2011, its top three priorities were, in order, counterterrorism, counterintelligence, protection from cyber-attacks and high-technology crimes. Many agents were transferred from ordinary criminal work to counterterrorism. There was a parallel steep decline in criminal case openings and convictions. There are now Joint Terrorism Task Forces in 104 cities nationwide. Of these, 71 were created after 9/11 and at 4000, manpower is "more than four times the pre-9/11 total."[54]

6.3 Untruth and unique definitions

As is well known, from 2006 on, Attorney General Alberto Gonzales, former Director of the NSA General Michael Hayden; his successors at NSA; Director of US National Intelligence, James Clapper; and other Administration, Congressional and Intelligence officials have ***actively misled*** the public about the extent of the NSA collection, or have flat-out lied, even under oath.[55] None have ever been punished, because this is clearly a concerted campaign of over a decade, blessed at the highest levels of the Executive and Congress.

The NSA likes to pretend that it cannot readily ***separate out domestic communications*** from foreign content, so it must somehow estimate the probability that a communication may be domestic, and it is given large latitude for mistakes. Yet with telephone calls in particular, for most calls this cannot be true. Certainly, it is untrue for landlines. Telephone calls have to get to a particular telephone in a particular country, via an assigned telephone number based on international standards. Metadata, with supporting technology available to the NSA, even before 9/11 sorted out protected domestic calls from foreign calls with an extremely high accuracy rate.

Landlines are simple, but a US resident using a US cellphone when traveling abroad, or a criminal buying a US cellphone to evade US collection abroad, can make things a little more complicated. A person using a US cellphone number in a foreign land can be forced to pay high fees or roaming charges, which itself could be a 'red flag'; however, one can now utilize an in-country SIM card to lower charges. A cellphone contacts the nearest cell tower to send and receive

[50] Oversight of the Federal Bureau of Investigation, Hearing before the Committee on the Judiciary, United States Senate, March 30, 2011, Serial No. J-112-12, S. Hrg. 112–173. Found at https://fas.org/irp/congress/2011_hr/fbi.pdf See p. 13 of the transcript (overall report p.17). Emphasis added.

[51] JTTFs are explained at https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces

[52] Oversight of the Federal Bureau of Investigation, Hearing before the Committee on the Judiciary, United States Senate, March 30, 2011, Serial No. J-112-12, S. Hrg. 112–173. Found at: https://fas.org/irp/congress/2011_hr/fbi.pdf See p. 13 of the transcript (overall report p.17). Emphasis added.

[53] Ibid., pp. 52 transcript/56 overall.

[54] Ibid., question for the record from Senator Hatch, pp. 63–64 and 66–67. Especially since the FBI has prevented few or no previously planned terrorist attacks, it has been argued that far more lives could be saved by tracking down the many unsolved murder cases than to have switched this extreme focus to counter-terrorism. Michael German, who worked in counter-terrorism for 12 of his 16 years at the FBI, makes this argument. See, e.g., "Former FBI Agent Mike German Talks About the NSA," ACLU, November 5, 2013, https://www.aclu.org/blog/former-fbi-agent-mike-german-talks-about-nsa?redirect=blog/national-security/former-fbi-agent-mike-german-talks-about-nsa

[55] See, for instance, Clapper's denial that NSA was collecting on millions of Americans before Snowden documented the opposite, at Andrew Rosenthal; "Making Alberto Gonzales Look Good," New York Times, Taking Note, 11 June 2013 AND Jennifer Granick; "NSA, DEA, IRS Lie About Fact That Americans Are Routinely Spied On By Our Government: Time For A Special Prosecutor," FORBES, 14 August 2013 https://www.forbes.com/sites/jennifergranick/2013/08/14/nsa-dea-irs-lie-about-fact-that-americans-are-routinely-spied-on-by-our-government-time-for-a-special-prosecutor-2/#78f9e7d19e8c AND Faiz Shakir; "The Hayden Record: Condoning Torture, Destroying Evidence, Misleading Congress," Think Progress, 8 December 2008 https://thinkprogress.org/the-hayden-record-condoning-torture-destroying-evidence-misleading-congress-676b2258b9fa

a signal, so cellphone metadata collected by NSA can geolocate the user as being currently in the US or abroad, which narrows the problem considerably. All US and foreign phones have a country designation as well an area code; so while there may be more difficult outlier cases, the main job of sorting out US phone calls becomes straightforward overall. Metadata cannot be encrypted, because if it were, the call wouldn't get to its intended destination and it would be difficult to keep billing records.

Snowden documents indicated that the NSA congratulated itself on picking up every single communication from six individual countries, with a seventh under development in 2013. If NSA can identify all those communications by country of origin, why can't it identify domestic US communications? And FBI Director Mueller's testimony, discussed above, seems to verify that the NSA has long sorted out, and promptly sent to the FBI, emails pertaining to the FBI's homeland jurisdiction [presumably including those emails in which one or both parties are in the US].

One relatively unknown, but very important example of misleading or false statements has been ***redefining*** "***collection***"[56] from its normal meaning and its prior intelligence community definition. In public, officials often now use the word to mean that collection does *not* occur when the data is scooped up and deposited in a database. Rather, the data is said to be "collected" only if, and when, an analyst retrieves particular communications from vast databases and actually looks at them - or, in prior intelligence vernacular, "analyzes" them. Thus, NSA can scoop up all US metadata and content, as well as other huge private and federal databases, store it all indefinitely, and perform automated pattern recognition on it - but still claim it has "collected" almost none of it. Despite this, Congressional legislation allegedly aiming to circumscribe NSA activities still fails to define "collection," as well as many other key terms, some of them also manipulated for disinformation.

The NSA also insists that only domestic metadata has been collected, and not telephone, email or other ***message content***. It is notable that spokespersons often carefully try to limit this and other claims to specific programs publicized via Snowden revelations, rather than applying the claims to NSA activities as a whole. As Edward Snowden revealed, the NSA has hundreds of programs.

Many of these programs are for foreign collection; but as discussed above, the NSA appears to get a lot of its domestic collection from abroad, or from targeting foreign communications on fiber optic lines traversing the US, which also carry US computer and telephone communications.

Sources[57] told this author in 2002 that domestic content was being collected. In 2016, when the government returned some email files - seized previously from the author's computer during a 2007 FBI raid - some email content through early 2016, nine years after the seizure, was returned. In January 2013, a US federal court had been informed that this author no longer was under US government investigation, but clearly NSA continued to collect both the metadata and content of her emails, at minimum. Edward Snowden has also insisted that domestic content is collected *en masse.*

A 2013 NSA Inspector General letter confirmed that in a dozen cases, NSA employees had spied on people of romantic interest to them.[58] What was not highlighted in this "LOVINT" scandal was that employees had access to both the metadata and content of these US persons' communications. Nor did most media point out that these people were caught mainly during periodically scheduled polygraph tests, rather than through ongoing supervision.

The NSA's claim that it does not collect domestic content also defies facts on the ground: since 9/11, NSA has built millions of square feet of data storage in San Antonio, Texas; Bluffdale, Utah; and Ft. Meade, Maryland (NSA Headquarters), even as steadily advancing technology permits highly dense storage in ever-smaller spaces. Metadata storage takes a relatively tiny space, just one moderately sized room for the entire world, according to William Binney; Binney and Edward Loomis first designed and built the NSA systems for digital data processing, storage, analysis, and retrieval. Some of this huge floor space is devoted to purposes such as decryption of content, NSA claims. But the great amount is assumed to be for storing communications intercepts.[59] Content, especially video and voice, takes enormously greater storage space

[56] Cushing, Tim; "Executive Order 12333 Documents Redefine 'Collection,' Authorize Majority Of Dragnet Surveillance Programs," TechDirt, 29 September 2014 https://www.techdirt.com/articles/20140929/13451828665/executive-order-12333-documents-redefine-collection-authorize-majority-dragnet-surveillance-programs.shtml The article is based on documents from an ACLU FOIA lawsuit discussed at Abdo, cited previously [Abdo, *Supra*, note (xi)]

[57] For the purpose of this writing, these sources cannot be revealed, or discussed herein

[58] See, e.g., Cyrus Farivar; "LOVEINT: On his first day of work, NSA employee spied on ex-girlfriend," arsTECHNICA, 27 September 2013 https://arstechnica.com/tech-policy/2013/09/loveint-on-his-first-day-of-work-nsa-employee-spied-on-ex-girlfriend/

[59] The San Antonio facility was billed as mostly for data storage, and the huge Ft. Meade facility, twice the size of Bluffdale, was presumed largely for the same purpose. Bluffdale has received most of the attention. A "leaked" floorplan indicated that little of it is devoted to data storage, but its first manager indicated that it was a data mart. **SEE** Howard Berkes, "Booting Up: New NSA Data Farm Takes Root in Utah," all tech considered, 23 Sept. 2013, http://www.npr.org/sections/alltechconsidered/2013/09/23/225381596/booting-up-new-nsa-data-farm-takes-root-in-utah; **AND** Sophie Curtis, "Leaked blueprints of NSA data storage facility reveal 'less capacity than thought.'" The Telegraph, 25 July 2013; **AND** With a flush budget, NSA has expanded facilities at additional known sites, and these could include data storage areas.* *Storage could be expanded at other collection sites for a distributed approach that would reduce risk from attack or other loss.

than metadata. Much of the content is foreign, but for the Section 702,[60] E.O. 12333,[61] domestic fiber collection, and the transferred GCHQ data, domestic and foreign material is collected, and may be stored, together. Regardless, even segregated domestic data, including phone, fax, email and other computer content, also is stored for five to six years, and longer if a person is considered suspect. If NSA cannot segregate domestic and foreign data, one wonders how they can meet court-mandated destruction deadlines.

7 "Collect it all:" does it deliver on the promise?

The US and other governments have imposed a Faustian bargain: sacrifice your privacy - and eventually your freedom – for security from domestic terrorism. Despite widespread unease when the New York Times and Edward Snowden revealed the actual terms of that US bargain, the issue no longer resonates in the US political landscape. Many US 'Progressives,' and US 'Tea Party conservatives,' strongly oppose mass surveillance. However, their differences on other issues appear to override cooperation on this one. Ultimately, since both Donald Trump and Hillary Clinton supported surveillance, there was no option for voters who sought a policy reversal. In the US, Democrats, Republicans, Congressional leadership, the Administration, and large media have all buried it as an issue. Memories are dim, and few are educated on the details.

Can and will the politicians keep their promise? Will we at least win security in exchange for losing our country? Will terrorism be defeated by this means? To date, there is minimal indication that our sacrifices of principle will pay off. These vast databases cataloguing our activities and private lives have largely failed to do what we were told domestic surveillance could do – *provide the very first, timely alert and tipoff of a pending attack, most especially about a* "*lone wolf*" attacker unconnected to a terrorist organization.

STELLARWIND, as the overall mass surveillance program originally was named, might provide that information more quickly and fully *after* an attack, or after a tip from elsewhere on whom to investigate. At this point, normal police work might come up with much the same. However, even in some cases where we had plenty of tipoff, the program did not prevent a pending attack.

After Major Hassan killed fellow soldiers at Fort Hood in 2009, plenty of evidence surfaced that his colleagues were alerted to his radical Islamist views. The FBI database even had his emails to a radical cleric[62] abroad who was closely followed by US Intelligence. Similarly, in 2001 the main NSA database had information that two of the 9/11 hijackers who had arrived in San Diego were in touch with a known Islamist safe house in the Middle East. But in both cases, the information was buried deep in the database and almost inexplicably ignored. It was also politically incorrect for the Army to investigate a radical Muslim. The FBI database apparently was too classified, too complicated and too large to spot the emails. The Hassan test case should have showcased STELLARWIND; instead, 12 people were killed and 31 injured. Similarly, the CIA had warnings from the father of the would-be 2009 airplane bomber discussed above, Abdulmutallab, but was so overwhelmed with huge amounts of data and thousands of leads that there was no follow-up, that would have spotted his booking in the airplane travel database of foreign arrivals.

Some believe there are too few terror attacks to provide the statistical basis to find predictive patterns that profile terrorists.[63] As both NSA veterans and the Snowden documents have contended, the result, instead, is that analysts are completely overwhelmed with irrelevant data.

A fiber optic information deluge already challenged NSA's pre-9/11 capabilities before further communications growth, the Internet explosion, and STELLARWIND's vast additions. By 2001, one group of NSA developers aspired to "own the web," apparently by collecting anything and everything. Another group contended that the only way to deal with the huge spigot was to automatically look at the metadata and key words in every communication available, but to collect and keep only communications information considered most likely to contain targets, or their associates. The goal of the latter was to *winnow down continually* the suspected targets through pattern and link analysis of the targets' immediate social networks, their web searches, chats, etc. This way, NSA and its partners could build upon legitimate suspicion, clues, and analysis (including non-communications sources), rather than trying to perform pattern and link analysis related to the personal activities of the entire US population, and almost the entire world population.

NSA's frequently and publicly repeated phrase, "collect it all" was the favored option. Such collection buries desired information in mountains of superfluous chaff. To use the government's constant analogy, if you are looking for a few needles in a haystack, it is counterproductive to keep piling on more hay. NSA would reply that they might miss something, including some of the needles, but better it is to find a few needles that often will lead to others, than to find none at all.

The 2013 Snowden papers confirmed the NSA strategic error by publishing internal NSA laments about being buried in excessive amounts of information. The FBI, to whom this

[60] See discussion within Section 3.3 of this article

[61] See discussion within Section 3.2 of this article

[62] FBI testimony, *supra*, note (xlv) plus ACLU, "Unleashed and Unaccountable," *op. cit.,* p. 24

[63] See Angwin, op. cit., and ACLU,"Unleashed and Unaccountable," *op. cit.,* p. 20.

untidy jumble is transferred, suffers the same fate. More than four years after 9/11, when the New York Times and then USA Today published their first reports on domestic surveillance, FBI sources complained to the Times about the huge number of pointless investigations that the NSA had spawned.[64] Seven years later, in 2013, the Judiciary Committee's Senator Patrick Leahy was very worried about finding an effective way to manage the extraordinary amount of data that is gathered by the FBI – "like a tsunami."[65] A George Washington University study of US states and local/municipal police organizations who received FBI "suspicious activity reports" from massive FBI databases, labeled them as a source of "white noise" that impeded effective intelligence analysis.[66]

The FBI and the national security establishment have long justified mass surveillance by proposing the need to find the "lone wolf" who is self-motivated and is largely unconnected to known terrorist groups. Former Director Mueller testified in 2013 that the "lone wolf" problem remained his greatest counterterrorism concern.[67] This risk has been oft cited, before and since, to alarm the public and justify invasive laws; and yes, the West has indeed suffered such attacks.

But, in the same breath during his testimony, Mueller said he was concerned because the "lone wolf" does not communicate with others,[68] and for that reason is the hardest to track. He admitted that the "lone wolf" provision of the USA PATRIOT Act had never been used, but wanted to retain it.[69] If these isolated individuals do not communicate about their terrorism plans, how could massive communications databases containing most US communications be expected to 'pop out' their identities? How could the government collect enough information to establish a terrorist profile, even with addition of databases on everything else - our purchases, finances, medical condition, licenses, etc.?

The "lone wolf" fixation appears to have served mainly to launch sting operations that encourage, enable and then nab those who are angry with the US and express it, or to stop those who travel to areas controlled by Islamic fundamentalists. The former do not represent a pending attack and, surely, there are more refined ways to catch the latter. The evidence indicates that mass domestic surveillance is a largely useless infringement on our First Amendment right to free speech, and our Fourth Amendment freedom from unreasonable search. How can STELLARWIND's great expense and obvious risks to civil liberty and our political system be rationalized on this basis?

On the rare occasions when the US government has been under serious pressure to justify domestic mass surveillance, after the New York Times and Snowden revelations of 2005 and 2013, it has alleged that the programs were instrumental in stopping pending attacks. However, the statistics did not hold up to scrutiny. Both times the administration claimed over 50 examples, about a dozen of them domestic, and administration and congressional supporters made sure these figures were widely publicized. However, in 2006, after further scrutiny it was found that domestic surveillance made a partial contribution to only one case. In 2013, the dissembling was repeated.[70] Intelligence deemed critical in several cases could have been secured with a warrant available under pre-9/11 procedures. Only four of the cases were made public, and investigation showed that they did not hold up. Many were not even planned attacks, including some that involved transfer of relatively small amounts of money to terrorist organizations, plus numerous FBI sting operations. The standard used was an alleged "contribution" to a case; this is far from the administration's own standard of providing a vital first tip-off of pending attack.

Moreover, by mid-2015 there had been 40 US alerts of potential pending attack over the past 14 years, all of them false alarms. Not a single attack was predicted or foiled.[71]

In a strongly worded opinion, Judge Richard Leon struck down the nationwide telephone metadata collection, with its "almost-Orwellian technology," as a likely violation of the Fourth Amendment ban on unreasonable search. Judge Leon observed that he had received not a single legitimate case supporting its efficacy, the same judgment expressed by a separate White House panel.[72] The administration had long claimed the program was vital to US safety.

The inability of these programs to provide a legitimate warning or to prevent any pending domestic terror attack over

[64] Lowell Bergman et al., *supra,* note (xliv)

[65] Oversight of the Federal Bureau of Investigation, Hearing, *op. cit.,* (note xlv) transcript pp. 9–10 (overall report pp. 13–14)

[66] ACLU, "Unleashed and Unaccountable," *op cit.,* p. 20.

[67] Oversight of the Federal Bureau of Investigation, Hearing, *op. cit.,* (note xlv) transcript pp. 8 and also 11(overall pages 12 and 15)

[68] *Ibid*

[69] Ibid., transcript p. 11 (overall p. 15). For a discussion of the provision, which allows FISA collection, even if a suspected terrorist is not connected to a foreign power, see Mary DeRosa, "Lone Wolf," Patriot Debates, American Bar Association blog, http://apps.americanbar.org/natsecurity/patriotdebates/lone-wolf

[70] Elliott, Justin and Theodoric Meyer, "Claim on "Attacks Thwarted" by NSA Spreads Despite Lack of Evidence," ProPublica, 23 Oct. 2013 https://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence AND Cohen, Cindy and DIA Kayyali, "The Top 5 Claims that Defenders of the NSA Have to Stop Making to Remain Credible," Electronic Frontier Foundation, 2 June 2014 https://www.eff.org/deeplinks/2014/06/top-5-claims-defenders-nsa-have-stop-making-remain-credible

[71] Johnson, Adam, "Zero for 40 at Predicting Attacks: Why Do Media Still Take FBI Terror Warnings Seriously?" FAIR, 1 July 2015 http://fair.org/home/zero-for-40-at-predicting-attacks-why-do-media-still-take-fbi-terror-warnings-seriously/

[72] Ellen Nakashima and Ann E. Marimow, "Judge: NSA's collecting of phone records is probably unconstitutional," Washington Post, 17 Dec. 2013 http://apps.washingtonpost.com/g/page/world/federal-judge-rules-nsa-program-is-likely-unconstitutional/668/ AND Isikoff, Michael, "NSA program stopped no terror attacks, says White House panel member," 20 Dec. 2013, http://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588

the last 15 years testifies volumes to the failure of the "collect it all" approach. A massive amount of money has been wasted. Most devastating and ominous of all, these programs have corroded our freedoms, our trust in government, the Constitution's Bill of Rights and US democratic institutions.

8 Persons of interest and the persecuted

Reporters are among those who have become "persons of interest" to the FBI – those individuals believed to be possibly involved in a crime, but who have not been charged or arrested. Aware that its questionable policies certainly would motivate leaks, after 9/11 the Executive Branch covertly turned to monitoring reporters. Cases have surfaced in which many US reporters admittedly have been electronically tracked.[73] This is to help forestall, identify and punish either whistleblowing or leaking of intelligence information, most especially the post-9/11 programs of dubious constitutionality.

When New York Times reporter James Risen for over seven years was threatened with jail because he refused to reveal his sources, previously accepted press freedoms were further abandoned.[74]

In addition to monitoring reporters, the US Intelligence Community created an Insider Threat Program,[75] to prevent espionage and preclude leaking and embarrassing public whistleblowing. Executive Order 13587[76] tightening internal security was issued in October 2011, after public revelations from Bradley/Chelsea Manning between April and November of 2010. Security, especially at the NSA, was intensified further after Edward Snowden's revelations beginning in June 2013.

When queried at an April 2014 briefing of the Senate Judiciary Committee about the need to distinguish legitimate whistleblowers from spies, the FBI walked out.[77] Previously, the FBI refused to provide the Committee their training manual on how to distinguish spies from whistleblowers. Whistleblowers, they said, would be protected if they "registered" as such. But internal objections to questionable practices, including official complaints to Inspectors General, have been an invitation to investigation and worse. The FBI has a "notorious" record of suppressing internal and other government whistleblowers.[78]

The main goal of the crackdowns has been to snuff the flow of published information about illegal domestic surveillance, torture, ill-conceived and dangerously awry operations, or other questionable, hidden or embarrassing activities. Any alleged leakers or whistleblowers are prosecuted under the 1917 Espionage Act, that allows no "public interest" defense and imposes draconian penalties. "The irony is obvious. The same people who are building a ubiquitous surveillance system to spy on everyone in the world, including their own citizens, are now accusing the person who exposed it of 'espionage,'" wrote Glenn Greenwald,[79] who reported on some of the Snowden documents. President George W. Bush began some investigations. By 2014, President Barack Obama indicted seven whistleblowers under the Espionage Act, compared to four pursued for leaking during the entire prior history of the 1917 act.[80] This was despite President Obama's Executive Order on classification that explicitly bars classification to cover up illegal, inefficient, or embarrassing Executive actions.[81]

A particular, emphasis was placed on finding the sources for the 2005 New York Times revelations on domestic surveillance and, following Edward Snowden's 2013 documentation of the NSA's astronomically greater excesses, to capture and prosecute Snowden and other whistleblowers. Not only is privacy under attack, but also those who object to attacks on privacy and civil rights, whether they do so through official channels (as with this author) or otherwise. These are the persecuted.

Suspected whistleblowers, with little organized public support and no in-house lawyer rising to their defense, face worse

[73] ACLU, "Unleashed and Unaccountable," *op cit.,* pp.32–33, AND The Committee to Protect Journalists, "Leak investigations and surveillance in post-9/11 America," October 2013. https://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php

[74] Sarah Ellison; "What was *New York Times* Reporter James Risen's Seven-Year Legal Battle Really For?" *Vanity Fair*, April 2015. http://www.vanityfair.com/news/2015/03/james-risen-anonymous-source-government-battle

[75] Carol D. Leonnig, Julie Tate and Barton Gellman; "U.S. intelligence agencies spend millions to hunt for insider threats, document shows," Washington Post, 1 Sept 2013 https://www.washingtonpost.com/politics/us-intelligence-agencies-spend-millions-to-hunt-for-insider-threats-document-shows/2013/09/01/c6ab6c74-0ffe-11e3-85b6-d27422650fd5_story.html?utm_term=.4d3d8af68fbd

[76] "Executive Order 13587 – Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information" White House, Washington, DC., 7 October 2011 [https://obamawhitehouse.archives.gov/the-press-office/2011/10/07/executive-order-13587-structural-reforms-improve-security-classified-net]

[77] Mike Masnick; "FBI Abruptly Walks Out On Senate Briefing After Being Asked How 'Insider Threat' Program Avoids Whistleblowers, Techdirt, 14 Apr. 2014 https://www.techdirt.com/articles/20140412/07290526888/fbi-abruptly-walks-out-senate-briefing-after-being-asked-how-insider-threat-program-avoids-whistleblowers.shtml

[78] ACLU, "Unleashed and Unaccountable," *op cit.,* pp. 30–32

[79] Daniel Politi; "Obama Has Charged More Under Espionage Act Than All Other Presidents Combined," Slate, June 22, 2013 http://www.slate.com/blogs/the_slatest/2013/06/22/edward_snowden_is_eighth_person_obama_has_pursued_under_espionage_act.html

[80] Jon Greenberg; "CNN's Tapper: Obama has used the Espionage Act more than all previous administrations, 10 January 2014 http://www.politifact.com/punditfact/statements/2014/jan/10/jake-tapper/cnns-tapper-obama-has-used-espionage-act-more-all-/

[81] "Classified National Security Information" [Executive Order 13526], White House, Washington, DC, January, 2010 https://www.ise.gov/resources/document-library/executive-order-13526-classified-national-security-information (Sec. 1.7. Classification Prohibitions and Limitations. (a) In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to: (1) conceal violations of law, inefficiency, or administrative error; (2) prevent embarrassment to a person, organization, or agency; (3) restrain competition; or (4) prevent or delay the release of information that does not require protection in the interest of the national security.)

prospects than reporters, especially under the Espionage Act. Even if whistleblowers are not guilty, are not convicted, and are not forced - under threat of lengthy prison sentence - to plead guilty whilst innocent, Intelligence Community employees receive the intended message: this will happen to them as well, should they speak up or be suspected of "leaking." Every Intelligence Community employee is now warned to report on the supposedly suspicious behavior of colleagues, and stands to be penalized if they did not do so. Under "continuous" monitoring, employees' workplace and personal electronic activities are reviewed.

Those objecting to seemingly illicit attacks on citizen privacy have been placed under prolonged siege that can ruin lives. For example, this author and four of her previously NSA-affiliated friends (Thomas Drake, William Binney, J. Kirk Wiebe and Edward Loomis) were wrongly accused of leaking part of the domestic surveillance program to the New York Times. There was no evidence supporting the accusations because, as reporter James Risen later said publicly, none of us were among his sources, and he did not even know us at the time. There was no evidence whatsoever to support the years-long investigations and the punitive indictment of Drake. Our sin was that, through established procedures, we dissented internally about domestic surveillance and about NSA's incompetence and waste of money. Drake and this author later exercised the First Amendment right to unclassified discussion with a reporter.

In our collective experience, suspected whistleblowers may:

- lack privacy during many years of surveillance (10 to 15 years in the case of this author), including electronic bugging and interference;
- have their home entered surreptitiously, without prompt notice, as (used to be) constitutionally required;
- be forced to pay for new electronics to replace those seized, plus for a destroyed replacement that was infected with a Trojan horse and key logger;
- have the case drag on for years while legal bills mount, and face an additional $1 million cost for a prospective trial phase, should one refuse to plea bargain (Thomas Drake was ruined financially and ultimately had to use a public defender);
- suffer family pain, discord, and break-up;
- witness destructive manipulation of offspring, to exert pressure on the parent;
- endure knowingly false and irrelevant public character assassination plus threats that the tactic would be repeated with a different spin;
- suffer trespass on home property, leaving items apparently meant to be seen;
- lose security clearances essential to one's profession and thus lose one's professional employment (regardless whether indicted and regardless of legal outcome);
- be raided by teams of FBI agents, perhaps even at gunpoint;
- be threatened as a group with "conspiracy," a charge often used to run up jail time, that can be based on the flimsiest of evidence - even a single suspect phone call - and that makes further group association and support dangerous;
- face falsified evidence on concocted alternative charges to force acceptance of plea bargains, after the original suspicions are dropped for lack of evidence;
- still be threatened with prison, including for one's remaining life;
- face prosecution for possessing unclassified documents that were retroactively classified (when other coercive tactics fail);
- discover that an Inspector General (an authority required to protect whistleblowers) will turn over whistleblower names to the FBI, and then destroy evidence that indicted whistleblower Drake was innocent of charges [an administration investigation and court case are underway];
- see ten felony charges dropped after classified pre-trial hearings, only four days before the public trial - a development the judge considered unprecedented and difficult to defend;
- be forced to get a court order to unseal affidavits that allegedly justified search warrants, after the investigation and court proceedings are finally over; and
- be forced to sue for return of seized materials, plus devote a large chunk of retirement to acting in court on these and other issues, as untrained *pro se*[82] attorneys.

NSA contractor Edward Snowden read about the indictment and persecution of Drake and acted accordingly. He has said that if there had been no Thomas Drake, there would have been no Edward Snowden. He connected with two reporters, took a trove of evidence documenting massive, shocking global attacks on the privacy of every individual at home and often abroad, and fled.

Whistleblowers, real or suspected, are not the only targets of the US government intimidation campaign against dissenters who object to its policies. On at least one occasion, a person who actively criticizes US foreign policy experienced what appeared to be obvious and otherwise unexplainable evidence of a home intrusion. On two other occasions, after he paused from his keyboarding, the computer continued to type things he had not written. Many FBI tactics appear to be for purposes of intimidation.

Some technology experts, in particular, have also had to endure the FBI's "***disruption activities.***" The targets often have been harmless hackers and IT professionals who act upon their

[82] Adjective or adverb \'prō-'sā, −'sē\, "on one's own behalf: without an attorney" https://www.merriam-webster.com/dictionary/pro%20se

opposition to domestic surveillance.[83] More cooperative hackers may be contracted by the government for its computer attack or other operations;[84] those who actively oppose US practices may instead find themselves to be under siege.

Personal electronics at the annual Defcon hacker conference have been monitored and misdirected. If an IT expert finds evidence of widespread hacking against a US corporation by an apparent government entity and prepares a speech revealing it, his hotel room may be ransacked and his car hit by thugs who try to lure him into an adjacent alley. If an expert spots software with a "back door" being used by the US government against citizens, and then publishes a patch to make the software secure, his professional equipment may be destroyed repeatedly, and his family's and communicants' electronics attacked as well. If one maintains a database on revelations and publications regarding the NSA, it may often be rendered inoperable, with vulnerability warnings also flashed to prospective site visitors.

A very qualified person can lose a job for no apparent reason and, surprisingly, fail to find another. Electronic job applications mysteriously arrive late, and the resume posted online is altered. The federal background investigation, required for many IT professionals, may have been seeded with unknown derogatory information, but it is impossible to acquire a copy of it, much as for years it was impossible to find out why one appeared to be on a "no-fly" list, or how to be taken off such a list. All these, and more, are real examples of a US government campaign against dissenters.

Although surreptitious, destructive government attacks have been quietly going on for years, electronic destruction has now been "legalized." As of December 2016,[85] a change to Rule 41 of the US Federal Rules of Criminal Procedure allows the government to secure even group warrants to attack and disable unidentified electronics belonging to unknown individuals. If one's computer has been taken over for a mass bot attack without one's knowledge, legally it can be destroyed. The equipment of private hackers investigating government hacking can be destroyed under cover of law. Congress failed to investigate, halt or even delay implementation of the measure, despite warnings from the IT community.[86]

Since 2009, the FBI's Counterterrorism Baseline Collection Plan has authorized agents to conduct "operations to effectively disrupt a subject's activities."[87] While this originally was publicized under the counterterrorism umbrella, authorities now include cyber security. In July 2016, Presidential Policy Directive 41, United States Cyber Incident Coordination, ruled that, due to its "expertise," the FBI would play a key role in coordinating agencies' "threat response" in the event of a significant attack, including identifying "disruption activities."[88] Extensive abuses, even killings, under disruption policy helped lead to the 1970s FISA law.

> "*This resurrection of reviled Hoover-era terminology is troubling, particularly because FBI counterterrorism training manuals recently obtained by the ACLU indicate the FBI is once again improperly characterizing First Amendment-protected activities as indicators of dangerousness.*" [89]

9 Conclusion

The vast and expanding breadth of the US government's surveillance into the personal details of citizens' lives is undeniable. Edward Snowden's 2013 revelations on classified intelligence collection are essentially undisputed and sometimes supported by later revelations. Since 2011, there has been exposure of other discreditable activities such as: additional secret means of domestic intelligence collection; amassing of business, government agency and other records; widening distribution of citizen information; systematic obstruction and lying to US courts and people; and reversion to disreputable FBI disruption operations. There is much evidence that such illegalities and privacy invasions have had minimal to no effect on security from domestic terror attacks.

With their copious information on most everyone in the US, American foreign and domestic intelligence agencies have amassed considerable concealed domestic political power. That influence can be exerted in circumstances of their choice, or at the choice of their informed political superiors. The ever-present danger is that such information will be used more or less ruthlessly to acquire and retain power, and thus to destroy our system of governance. We are at the fearful point where, now and in the future, we will have no sure answers to core questions that still are not being raised publicly. Who is really running this country? Who is deciding a given policy, for what motive, and to what purpose?

[83] For more on this, see Gary Chapman, "National Security and the Internet," LBJ School of Public Affairs, University of Texas, pp. 13 and 17 http://www.utexas.edu/lbj/21cp

[84] See, for instance, Stacy Cowley; "NSA wants to hire hackers," CNNMoney, July 29, 2012. http://money.cnn.com/2012/07/27/technology/defcon-nsa/

[85] See, for instance, Lisa Vaas; "Campaign's bid to delay Rule 41 'legal hacking' bill," *naked security by Sophos,* Nov. 21, 2016, https://nakedsecurity.sophos.com/2016/11

[86] Erin Kelly; "Congress allows rule permitting mass hacking by government to take effect," USA Today, 30 November 2016 http://www.usatoday.com/story/news/politics/elections/2016/11/30/congress-allows-rule-permitting-mass-hacking-government-take-effect/94683030/

[87] ACLU, "Unleashed and Unaccountable," *op cit.,* p. 13

[88] See the FBI press release at http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805 and text of the Presidential Policy Directive at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[89] ACLU, "Unleashed and Unaccountable," *op. cit. p. 13*

Most US citizens remain blithely unaware of the likely extent of their own dossiers. They probably will not grasp the full import of this situation until representative files are exposed publicly. For fear of citizen and legal backlash, the government cannot allow such exposure. In the public arena, the origin or existence of file content must be hidden or disguised, just as it has been in US courts. This reduces the overt utility of the information, but it can be useful in other ways. When undermining a political opponent, for example, intelligence agencies or government politicians could, without attribution, draw from information in the dossiers to tip off media to an embarrassing personal, business or family issue. The media might then be able to confirm it through investigative reporting. However, mounting a defense against public allegations, or "proving a negative," could require exposing the entire file. Therefore, these files are most useful for attack, or for unattributed "background" information that influences intelligence reporting and law enforcement investigations.

Illegal, unconstitutional activities have been disguised and protected for over 15 years by misdirection, lies, cover-up, and tolerance at the highest levels in all branches of US government. Inevitably, an entrenched culture of rot and corruption therefore has pervaded the Intelligence Community and its defenders. Eradicating this culture requires a grassroots movement that cleans out the Executive and Congress, and thereafter the Judiciary. There is safety in numbers – and in votes. The collected masses need a disruption strategy of their own. This task would be very far from easy, but the alternative scenario is grim.

Compliance with ethical standards

Conflict of interest The author declares no conflict of interest.

Funding There is no funding source for this article.

Ethical approval This article does not contain any data, or other information from studies or experimentation, with the involvement of human or animal subjects.

Informed consent Not Applicable.

References

1. Isikoff M. The whistleblower who exposed warrantless wiretaps. Newsweek 2008. http://www.newsweek.com/whistleblower-who-exposed-warrantless-wiretaps-82805.
2. Savage C. Declassified Report Shows Doubts About Value of N.S.A.'s Warrantless Spying. New York Times. 2015. https://www.nytimes.com/2015/04/25/us/politics/value-of-nsa-warrantless-spying-is-doubted-in-declassified-reports.html.
3. Dalberg-Acton JEE. Historical essays and studies. In: Figgis JN, Laurence RV, editors. London: Macmillan; 1907.
4. Abbey E. In: MaCrae J, editor. The serpents of paradise: a reader. New York: Owl Books/Henry Holt & Co.; 1995.
5. Barrett D. Gun-show customers' license plates come under scrutiny: federal agents enlisted local police to scan cars' plates at shows' parking lots. Wall Street J2016.
6. Hill K. E-Z passes get read all over New York (not just at toll booths). Forbes 2013. https://www.forbes.com/sites/kashmirhill/2013/09/12/e-zpasses-get-read-all-over-new-york-not-just-at-toll-booths/#1e1da53b62c0.