Part I

Surveillance Techniques and Technologies

1 NSA Surveillance in the War on Terror

Rachel Levinson-Waldman†

On March 12, 2013, Senator Ron Wyden of Oregon asked James Clapper, then-director of national intelligence (DNI), whether the National Security Agency "collect[s] any type of data at all on millions or hundreds of millions of Americans."[1] The question was posed during an open session of the Senate Select Committee on Intelligence, on which Senator Wyden sits. DNI Clapper paused and answered, "No … not wittingly." Three months later, the details of a highly classified program that collected the bulk telephone records of millions of Americans – a program about which Senator Wyden had been issuing cryptic warnings for nearly two years[2] – were published in the *Guardian* newspaper. A month after that, Clapper finally retracted his statement, saying that it was "clearly erroneous."[3]

When Clapper made his statement, Edward Snowden, soon to become the country's most famous whistleblower, was working as an National Security Agency (NSA) contractor with top-secret clearance. However, the regular sharing of raw data with foreign intelligence agencies – often with little oversight or effort to eliminate personally identifiable information found in Americans' private communications – had raised grave concerns for Snowden, and he had already begun questioning the legal and ethical implications of the NSA's secret intelligence operations.[4]

When he heard Clapper's answer, he decided to act. He shared a trove of documents with a set of international reporters, ultimately resulting in the disclosure of a variety of classified surveillance programs, including programs collecting and analyzing the content and metadata of Americans' phone calls and emails, email address books and instant messaging "buddy lists,"[5] and more. These disclosures would reshape both the public's understanding of the post-9/11 legal landscape and the legislative, executive, and judicial

† Senior Counsel, Brennan Center for Justice, Liberty and National Security Program.

1 *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 113th Cong. 66 (2013) (statement of Sen. Wyden, Member, S. Select Comm. on Intelligence).

2 *See, e.g.*, Charlie Savage, *Senators Say Patriot Act Is Being Misinterpreted*, N.Y. Times (May 27, 2011), at A17, http://www.nytimes.com/2011/05/27/us/27patriot.html.

3 Ryan Lizza, *State of Deception*, New Yorker (Dec. 16, 2013), http://www.newyorker.com/magazine/2013/12/16/state-of-deception.

4 James Bamford, *The Most Wanted Man in the World*, Wired (Aug. 22, 2014), https://www.wired.com/2014/08/edward-snowden/.

5 Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, Wash. Post (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

appraisal of the legal underpinnings of the surveillance programs. Understanding the magnitude and details of the programs that Snowden ultimately had a hand in revealing – the scope of this chapter – requires rewinding the clock almost twelve years.

I Secret Surveillance: 2001–2008

Less than a month after four planes were flown into the World Trade Center towers in New York City, the Pentagon in Washington, DC, and a field in rural Pennsylvania, President George W. Bush authorized the beginnings of what would become a sweeping mass surveillance program. It would swiftly outgrow even the modest limitations put upon it, ultimately becoming what the inspector general of the Department of Justice would call, in an exhaustive 2009 report, a "permanent surveillance tool."[6]

That top secret program, code-named STELLARWIND (hereinafter, Stellar Wind), involved an "unprecedented collection of information concerning U.S. persons."[7] It was eventually beset by legal and operational problems, some so significant that they prompted threats of mass resignations by top officials at the Department of Justice and FBI that would have eclipsed Nixon's Saturday Night Massacre.

Although no aspects of Stellar Wind remain in precisely the form in which they existed during the years after September 11, 2001, the program laid the foundation for the even more comprehensive surveillance programs that followed. For the last fifteen years, reams of information have been collected about Americans – in the name of fighting terrorism – and crunched using analytical programs looking for insights within the mass of data.

Some of those programs reportedly have been successful at fighting terrorism, though few details are publicly available; others are nearly universally agreed to have contributed little to keeping the nation safe.[8] Some programs have had shifting legal justifications, and some have been seemingly abandoned, only to reemerge under different auspices. And there are pieces that remain obscured behind redactions.

A *STELLARWIND*

1 Background

In the days after the September 11 attacks, U.S. officials scrambled to try to figure out how they had missed the largest attack on American soil since Pearl Harbor. On October 4, 2001, President George W. Bush issued a "highly classified presidential authorization"[9] finding that the September 11 attacks constituted an "extraordinary emergency" and authorizing the NSA to collect warrantlessly three broad categories of signals intelligence: the content of specified "Internet communications" and telephone calls, metadata

6 Offices of the Inspectors Gen. of the Dep't of Def. et al., (U) Annex to the Report on the President's Surveillance Program 396 (2009), https://oig.justice.gov/reports/2015/PSP-09-18-15-vol-III.pdf.

7 *Id.*

8 *See, e.g., id.* at 397, 399; *see also id.* at 401 ("[A]lthough Stellar Wind information had value in some counterterrorism investigations, it generally played a limited role in the FBI's overall counterterrorism efforts.").

9 Privacy & Civil Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 16 [hereinafter PCLOB Report on 702] (2014), https://www.pclob.gov/library/702-Report.pdf.

about specified Internet communications, and metadata about specified phone calls.[10] ("Metadata" is data about data – in this case, not the content of the communications, but information *about* those communications, such as when they occurred and who was involved.) The program was referred to both by its code name, Stellar Wind, and by the umbrella term "President's Surveillance Program."

Under Stellar Wind, both content and metadata could be gathered when at least one of the parties to the call or email was outside the United States and was "reasonably believed to be associated with any international terrorist group."[11] In addition, metadata for any Internet communication or phone call could be collected if none of the participants was a US citizen, if at least one person was outside the United States, or if there was "reasonable articulable suspicion to believe the communications related to international terrorism."[12] In other words, if one person *was* inside the United States (but the other was not), or if *all* persons were inside the United States (but they were not U.S. citizens), then metadata about their communications could be gathered, even if their communications had nothing to do with international terrorism.

Once the metadata had been assembled into a database, it could be searched using a phone number or email address (an "identifier") for which there was "reasonable articulable suspicion" (RAS) to believe that the identifier "had been used for communications related to international terrorism."[13] These identifiers were called "seeds" or "selectors." Notably, the determination that a particular seed met the RAS standard occurred inside the NSA, without external oversight.[14]

Absent the emergency declared by President Bush, the data collection – at the very least the collection of content – would have required permission from the Foreign Intelligence Surveillance Court. Instead, as each presidential authorization expired,

[10] *See, e.g.*, Charlie Savage & James Risen, *New Leak Suggests Ashcroft Confrontation Was over N.S.A. Program*, N.Y. Times, (June 28, 2013), at A6, http://www.nytimes.com/2013/06/28/us/nsa-report-says-internet-metadata-were-focus-of-visit-to-ashcroft.html. "Internet communications" included emails and Internet phone calls such as Skype (otherwise known as VoIP) that crossed the data links of AT&T, MCI/Verizon, and Sprint. *See, e.g.*, Barton Gellman, *U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata*, Wash. Post (June 15, 2013), https://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html. They may have also included "Chat – video, voice, Videos, Photos, Stored data, … File transfers, Video Conferencing, Notifications of target activity – logins, etc., [and] Online Social Networking details." *See* Presentation, Special Source Operations, Nat'l Sec. Agency, Slide 4, (Apr. 2013) http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document. It is not clear which, if any, of these types of communications beyond email and VoIP were also a part of the collection under Stellar Wind.

[11] Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 388. Note that the program is variously described as requiring "reasonable belief" or "probable cause." *See, e.g., id.* at 361. In March 2004, Deputy Attorney General Jack Goldsmith objected to the "any international terrorist group" standard on the grounds that the targeted group was too broad. President Bush then limited the content collection to communications for which at least one person was reasonably believed to be a member of al Qaeda or associated forces. Charlie Savage, Power Wars: Inside Obama's Post-9/11 Presidency, 191–192 (2015).

[12] *See* Benjamin Wittes, *The NSA IG Draft Report: An Analysis, a Question, and a Possible Answer*, Lawfare (July 16, 2013, 10:01 PM), https://www.lawfareblog.com/nsa-ig-draft-report-analysis-question-and-possible-answer; Office of the Inspector Gen. of the Nat'l Sec. Agency, ST-09-002 Working Draft (2009), http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.

[13] Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 55.

[14] *Id.* at 55 (describing process of shift coordinator's review and approval).

White House officials reassessed whether there were facts demonstrating a continued threat of terrorist attacks in the United States.[15] Once the standard was satisfied, the attorney general, with the advice of the Department of Justice's (DOJ) Office of Legal Counsel, signed the authorization attesting that the activities were legal and satisfied the Fourth Amendment's reasonableness requirement.[16] The memos also directed that information about American citizens be minimized, as long as the minimization was "consistent with the object of detecting and preventing terrorism."[17] Once the authorization was in place, the program was renewed for another thirty to sixty days.

As would later be revealed, however, the NSA secretly interpreted its already broad authorization in two ways in order to engage in even more intrusive collection and analysis. First, instead of limiting the categories of metadata to those described in the presidential authorization, it collected phone and email metadata in bulk, to create "a database from which to *acquire* the targeted meta data."[18] The agency then used the RAS standard to determine what searches it could run in the database.[19] It justified this practice on the dubious theory that it did not "acquire" the data until it ran searches, so it could vacuum up huge quantities of information without triggering the language of the presidential authorization.[20]

Second, the NSA crafted a separate "alert" system that operated outside the RAS process for the telephony metadata program. For two years, NSA analysts queried the telephony metadata not only with RAS-approved selectors but also with phone numbers that were simply "of interest" to the analysts.[21] When the selectors produced a hit against the metadata database, the analysts would then look more closely to determine whether the RAS standard was satisfied and contact chaining thus permitted.[22] The existence of this procedure emerged during a briefing with the Department of Justice; because it diverged significantly from the representations the agency had made to the Foreign Intelligence Surveillance Act (FISA) court regarding its compliance with the

15 Office of the Assistant Attorney Gen., Memorandum for the Attorney General Re: Review of the Legality of the STELLAR WIND Program 9 (2004), https://fas.org/irp/agency/doj/olc/stellar.pdf.

16 Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 389.

17 Office of the Assistant Attorney Gen., *supra* note 15, at 7.

18 Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 49 (emphasis added).

19 *Id.* at 49. According to the Inspector General's report, because the RAS standard was applied to searches, the NSA only accessed a minuscule fraction of the data it obtained; "By the end of 2006, .001% of the data collected had actually been retrieved from its database for analysis." *Id.* at 50.

20 *See, e.g.*, Office of the Inspector Gen. of the Nat'l Sec. Agency, *supra* note 12, at 38 (observing that the NSA's Office of general counsel and the inspector general accepted the agency's explanation that it "did not actually 'acquire' communications until specific communications were selected. In other words, because the authorization permitted NSA to conduct metadata analysis on selectors that met certain criteria, it implicitly authorized NSA to obtain the bulk data that was needed to conduct the metadata analysis"); *see also* Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 108 n.123 ("The term 'acquired' was not clarified until the March 11, 2004, Presidential Authorization. That Authorization stated that meta data was 'acquired … when, and only when, the Department of Defense has searched for and retrieved such header/router/addressing-type information, including telecommunications dialing-type data (and not when the Department obtains such header/router/addressing-type information, including telecommunications dialing-type data … for retention).'") (part of final sentence redacted and internal quotation marks omitted).

21 Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 232–233.

22 *Id.* at 232.

RAS standard, the NSA ultimately shuttered it, and the FISA court imposed additional temporary checks on the agency's authority as described later.[23]

Although the program was originally intended to be a temporary response to the attacks, it soon became clear that the presidential authorizations would be renewed indefinitely.[24] Because a significant fraction of the world's phone calls, and an even more substantial number of the world's Internet communications, go through the United States, the secret presidential authorizations led to a surveillance bonanza for the NSA. As of 2003, more than 37 billion minutes per year of telephone communications – about 20 percent of the total worldwide – either began or ended in the United States.[25] (Another 23 billion minutes traversed the United States without beginning or ending inside the country; the NSA was authorized under a Reagan era presidential order, Executive Order 12333, to capture those calls.)[26] Through relationships with several telecom companies, the NSA could get access to more than 80 percent of those 37 billion minutes' worth of calls.[27] The United States' advantage when it came to Internet communications was even more striking: as of 2002, nearly 99 percent of the world's Internet bandwidth either began or ended in the United States.[28] From October 2001 through January 2007, when the last vestiges of the program were shut down (though reanimated elsewhere under various other authorities, as described later), nearly thirty-eight thousand email addresses and telephone numbers were tasked for content collection under Stellar Wind.[29]

2 Operational Details: Phone and Email Metadata Program

Once the presidential authorizations were in place, they were provided to telecommunications companies, which complied by providing information about their customers' communications.[30] Specifically, the companies – beginning with AT&T, Verizon, and BellSouth – forwarded "call detail records," or routing information that included the phone numbers on either side of a telephone call and the date, time, and length of each call, but not the content of the phone calls.[31] Similarly, the NSA received email metadata revealing the senders and recipients of emails, who was cc'd or bcc'd, and the dates and times those emails were sent (but not the body of the emails or the information in the "subject" or "re" lines).[32]

23 *Id.*; *see infra* section II(A).
24 Office of the Inspector Gen. of the Nat'l Sec. Agency, *supra* note 12, at 11.
25 *Id.* at 27.
26 *Id.*
27 *Id.*
28 *Id.* at 28 ("[D]ata available from 2002 shows that at that time, worldwide international bandwidth was slightly more than 290 Gbps [Gigabits per second]. Of that total, less than 2.5 Gbps was between two regions that did not include the United States.").
29 *Id.* at 15.
30 Lizza, *supra* note 3.
31 Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 49.
32 *Id.* at 51. It appears that the three main companies that provided their customers' email metadata were AT&T, MCI/Verizon, and Sprint. *See, e.g.*, Office of the Inspector Gen. of the Nat'l Sec. Agency, *supra* note 12; Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. Times, Aug. 16, 2015, at A1, http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0; Gellman, *supra* note 10.

Once the metadata had been processed into databases, NSA analysts looked for unknown or unexpected links to foreigners by "contact chaining," a process that uncovered "the contacts made by a particular telephone number or e-mail address . . . as well as contacts made by subsequent contacts."[33] NSA analysts tended to go out more tiers with phone numbers than with email addresses because phone calls generally were not made to multiple people at once, unlike spam emails.[34]

Notably, the NSA had requested permission to do contact chaining on Americans' data two years earlier, when alarm bells were ringing about threats from al Qaeda. Under that proposal, Americans' phone numbers would have been "masked," or hidden, unless the NSA received a warrant to uncover them. The Justice Department had refused permission, advising that analyzing Americans' phone records without a warrant was illegal.[35] In the aftermath of September 11, however, Vice President Dick Cheney approached General Michael Hayden, then the head of the NSA, to ask what the NSA could be doing if Hayden was given additional legal authority. Together, they renewed the earlier plan, but without the protections for Americans' information.[36]

3 Legal Reviews

Initially, there was no judicial review and little internal legal review of these authorizations. A month into the program, in early November 2001, then-Deputy Assistant Attorney General John Yoo issued a twenty-one-page memorandum that would come to be roundly criticized for its superficial legal reasoning and failure to represent the basic facts of the program accurately.[37] Although the text of the memo remains almost entirely classified by redaction, Yoo appears to have argued that Article II of the Constitution gives the president an inherent right, which cannot be infringed by Congress or otherwise, to "engage in warrantless searches that protect the national security."[38] Despite the fact that the Foreign Intelligence Surveillance Act expressly limited the president's authority to engage in wiretapping, Yoo asserted that Congress had not acted to restrict the president's authority in this realm.[39] He suggested that intercepting communications crossing into or out of the United States fell under the "border search exception" to the Fourth Amendment.[40] And because few people were read into the program[41] or had access to the legal memo approving it – even the NSA's general counsel was barred from reading it by Vice President Dick Cheney's legal counsel – there was little pressure to

33 Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 54.
34 *Id.*
35 Lizza, *supra* note 3.
36 Lizza, *supra* note 3.
37 Memorandum from John C. Yoo, Deputy Assistant Attorney Gen. to Attorney Gen. (Nov. 2, 2001), https://www.justice.gov/sites/default/files/olc/legacy/2011/03/25/johnyoo-memo-for-ag.pdf; Offices of the Inspectors Gen. of the Dep't of Def. et al, *supra* note 6, at 10–14.
38 Memorandum from John C. Yoo, Deputy Assistant Attorney Gen. to Attorney Gen., *supra* note 37, at 7.
39 Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 391.
40 Offices of the Inspectors Gen. of the Dep't of Def. et al., Unclassified Report on the President's Surveillance Program 12 (2009), https://fas.org/irp/eprint/psp.pdf.
41 "The process of being 'read into' a compartmented program generally entails being approved for access to particularly sensitive and restricted information about a classified program, receiving a briefing about the program, and formally acknowledging the briefing, usually by signing a nondisclosure agreement describing restrictions on the handling and use of information concerning the program." *Id.* at 10 n.10.

revisit its legal moorings. The program thus continued in its basic form (albeit with a few tweaks) for two and a half years, until the spring of 2004.

In December 2003 Yoo was replaced by Jack Goldsmith, beginning a four-year-long process of creating new legal analyses – and in some cases new statutes – to justify the three collection programs. When Goldsmith began reviewing the justification for the programs, he concluded that Yoo's legal reasoning was faulty in several respects, as described in more detail in the following, and that Yoo had failed to understand or accurately describe certain factual aspects of the government's surveillance program.[42] The Yoo memos therefore did not even fully cover Stellar Wind – meaning that the White House had been operating a secret mass surveillance program without adequate Office of Legal Counsel review or approval.[43] Goldsmith's attempts to flag the legal problems, and to bring the programs into basic legal compliance, sparked repeated skirmishes between the Department of Justice and the White House.

In March 2004, with the then-current presidential authorization slated to expire on March 11, the conflict came to a head. At Goldsmith's recommendation, Acting Attorney General James Comey (who later became head of the FBI) refused to recertify the program, and Attorney General John Ashcroft refused to overrule him from the hospital bed where he lay with acute appendicitis.[44] On March 11, the day the existing presidential authorization expired, White House Counsel Alberto Gonzales – at the direction of President Bush – certified the continuation of the phone metadata and content collection programs, without approval from the Department of Justice.[45] Two other aspects of Stellar Wind were the subjects of such serious conflict between the DOJ and the White House that one was retroactively authorized and the other temporarily shut down.

The aspect to be retroactively authorized was the NSA's practice, described previously, of collecting far more phone and Internet metadata than was permitted by the authorization, so the agency could later search through its bulk database for the information it was actually authorized to obtain. To "narrow the gap" between what the authorizations allowed and what the NSA was doing in practice, President Bush substantially changed the language of his March 2004 reauthorization and declared it to apply both prospectively and retroactively.[46] Now, in addition to being able to "acquire" metadata when at least one party to the communication was believed to be outside the United States or the message was linked to terrorism, the NSA was also explicitly authorized to "obtain and retain" any telecommunications metadata, including that of wholly domestic communications.[47] Because *collecting* metadata was redefined as "obtaining and retaining" the information, "acquiring" – the activity that was initially sanctioned and regulated by the authorization – was transformed into *querying* the collected metadata for communications involving foreigners abroad or linked to terrorism. In other words, the agency

42 Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 124.
43 *Id.* Notably, the information identifying the particular program that was not described accurately is redacted from the inspector general's report, though it appears that the problem may have been Yoo's failure to understand that Internet backbone providers do not process or retain email metadata, described *infra* Section I(A)(4). *See, e.g.*, Julian Sanchez, *Reading Goldsmith's STELLARWIND Memo (Part I)*, Just Security (Sept. 10, 2014, 5:05 PM), https://www.justsecurity.org/14789/reading-jack-goldsmiths-stellarwind-memo/.
44 Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 130–31.
45 Office of the Inspector Gen. of the Nat'l Sec. Agency, *supra* note 12, at 37.
46 Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 144.
47 *Id.* at 145.

could collect everything, with the limitations entering into effect only when the data was searched. And this new distinction was given retroactive effect, to sanction all the previous overcollection.[48]

The second part of Stellar Wind that came under fire was the Internet metadata program, which had precipitated much of the wrangling between the Department of Justice and the White House. As described later, Goldsmith appears to have concluded that the Internet metadata collection simply was not supported by the existing statutory scheme. The week after President Bush directed his White House counsel to recertify the other two programs on his sole authority, the president rescinded his authorization for the email metadata program, giving the agency "a week to stop collecting it and to block access to its existing database."[49] (This suspension would be short-lived, however, because the bulk of the program would ultimately be reanimated by the Foreign Intelligence Surveillance court under a new interpretation of a provision of FISA, as described later.) On May 6, 2004, Goldsmith submitted a memo to Ashcroft on the legality of the three collection programs, superseding Yoo's earlier memo.[50] Though significant portions of the memorandum are still classified, the memo, along with other sources, demonstrates how Goldsmith tried to shift the content and phone metadata pieces onto firmer ground, and also suggests why the Internet metadata piece provoked a near-crisis.

4 Legal Analysis

Similar to Yoo, Goldsmith took a broad view of the executive's inherent authority to collect foreign intelligence when it came to content collection. Unlike Yoo, however, he grounded it in the Authorization for Use of Military Force (AUMF), the Congressional enactment authorizing the president to go to war against any nations or organizations involved in the September 11 attacks.[51] In Goldsmith's view, because the AUMF authorized war, it also authorized the President to take related steps, including collecting signals intelligence – both content and metadata – about the enemy (even though one end of the communication was likely to be an American in the U.S.). The AUMF thereby took precedence over the otherwise applicable limitations in the Foreign Intelligence Surveillance Act, allowing the content collection program to pass statutory muster.[52]

With respect to metadata collection, however, the landscape was different. The government's bulk collection of metadata under Stellar Wind was explicitly designed to

[48] *Id.* at 146; *see also* Charlie Savage, *George W. Bush Made Retroactive N.S.A. 'Fix' after Hospital Room Showdown*, N.Y. Times, Sept. 21, 2015, at A13, http://www.nytimes.com/2015/09/21/us/politics/george-w-bush-made-retroactive-nsa-fix-after-hospital-room-showdown.html.

[49] Charlie Savage & James Risen, *New Leak Suggests Ashcroft Confrontation Was over N.S.A. Program*, N.Y. Times, June 28, 2013, at A6, http://www.nytimes.com/2013/06/28/us/nsa-report-says-internet-metadata-were-focus-of-visit-to-ashcroft.html.

[50] Office of the Assistant Attorney Gen., *supra* note 15. *See also* Offices of the Inspectors Gen. of the Dep't of Def. et al., *supra* note 6, at 186 (describing memo as "the most comprehensive assessment of the Stellar Wind program drafted by the Office of Legal Counsel"); *id.* at 392 (describing memo as superseding Yoo's earlier opinions).

[51] *See* Press Release, Office of the Press Secretary, President Signs Authorization for Use of Military Force Bill, Statement by the President (Sept. 18, 2001), https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010918-10.html.

[52] *See supra* note 11, regarding the narrowing of content collection so it collected only communications of members of the groups identified in the AUMF.

capture Americans' communications: unlike the content collection piece, it did not focus on the communications of the enemy. The AUMF therefore could not justify the collection of either phone or Internet metadata.

The phone metadata program was nevertheless deemed permissible. Because it involved the collection of existing records from the telecommunications companies, it did not actually constitute "surveillance" under FISA, and it therefore didn't need a statutory workaround. (As described below, it was also not seen as raising any constitutional issues.)

The Internet metadata program presented a graver statutory dilemma, however. It did count as surveillance under FISA, but the AUMF could not rescue it. FISA's definition of "electronic surveillance" includes the "installation or use" of any "device in the United States for monitoring to acquire information,"[53] and this is precisely how the email records were being obtained. Unlike phone companies, email providers do not generate records of email communications for billing purposes; instead, a device that logs email traffic must be installed on a network switch. The installation and use of such a device constitutes electronic surveillance under FISA, which required judicial approval. And because the AUMF only gave the President the authority to surveil "enemies" abroad, not Americans domestically, it could not override the executive's obligations under FISA.[54] Although the relevant part of Goldsmith's memo is redacted, this statutory tension strongly suggests that this is the reason the Internet metadata program was abruptly shut down in mid-2004; there was simply no legal justification for it in its existing form.

The memorandum also evaluated Stellar Wind's consistency with the Fourth Amendment. The closest the Supreme Court has come to addressing the question of constitutional authority for foreign intelligence collection was in the 1972 case *United States v. United States District Court*, commonly known as *Keith*.[55] The Court held in *Keith* that the Fourth Amendment's warrant requirement does apply to investigations of purely *domestic* threats to the nation's security, but reserved the question of whether a warrant was required for the President to exercise his or her *foreign* intelligence surveillance powers.[56] Notwithstanding that silence, the courts of appeals that have endorsed the President's inherent authority to conduct warrantless foreign intelligence surveillance have relied on *Keith* in reaching their decisions.[57]

Following and expanding their lead, the Goldsmith memo concluded that the President has inherent constitutional authority, consistent with the Fourth Amendment, to conduct warrantless searches for foreign intelligence purposes both in wartime and in peacetime, as Commander-in-Chief and as Chief Executive.[58] The memo depicted the arena of foreign intelligence collection as a case of "special needs beyond the normal

[53] 50 U.S.C. § 1801(f)(4).
[54] Julian Sanchez, *Reading Goldsmith's STELLARWIND Memo (Part I)*, Just Security (Sept. 10, 2014, 5:05 PM), https://www.justsecurity.org/14789/reading-jack-goldsmiths-stellarwind-memo/; *see also* Julian Sanchez, *What the Ashcroft "Hospital Showdown" on NSA Spying Was All About*, Ars Technica (July 29, 2013, 9:00 AM), http://arstechnica.com/tech-policy/2013/07/what-the-ashcroft-hospital-showdown-on-nsa-spying-was-all-about/.
[55] *United States v. U.S. Dist. Court* (*Keith*), 407 U.S. 297 (1972).
[56] *Id.* at 308.
[57] Office of the Assistant Attorney Gen., *supra* note 15, at 40.
[58] *Id.* at 37.