Testimony for the Privacy and Civil Liberties Oversight Board Forum:

USA Freedom Act: Lessons Learned and A Look Ahead

Susan Landau
Fletcher School of Law & Diplomacy and School of Engineering, Tufts University[1]

May 31, 2019[2]

Thank you for the opportunity to testify before the Privacy and Civil Liberties Oversight Board. I appreciate the opportunity to raise issues regarding efficacy of the USA Freedom Act before the board. My remarks are based on research conducted with Asaf Lubin, Cybersecurity Policy Fellow at the Fletcher School of Law and Diplomacy, Tufts University.[3]

In the months before the 9/11 attacks, several crucial pieces of evidence were missed. One was a set of calls made between an apartment in San Diego, California and a Yemeni number known to be a safe house for an al Qaeda operations center in Sana.[4] The NSA had been listening in to satellite calls connecting to the Yemeni number. But because NSA did not have access to the switch or Call Detail Records (CDRs), the agency was not privy to information revealing the location of the other end of the call. It was this intelligence fault that triggered the desire for the telephony metadata program. As former NSA Director Michael Hayden later lamented, "If we had the 215 program at the time, we would have thrown that selector at that mass of American phone bills and phone connection and said, "Did anybody here talk to this number in Yemen?" and ka-jink! The San Diego number would have popped up."[5]

---

[1] Affiliation for identification purposes only.

[2] Revised and submitted July 22, 2019.

[3] This testimony is part of a project funded by the William and Flora Hewlett Foundation under grant 2018-7277.

[4] DOES STATE SPYING MAKE US SAFER: THE MUNK DEBATE ON MASS SURVEILLANCE, at 25 (RUDYARD GRIFFITHS ED., 2014).

[5] *Id.*, at pp. 25-26.

Shortly after the attacks, President George W. Bush directed the Secretary of Defense to start a program of collecting, in bulk, metadata from telephone and Internet communications.[6] For six years, the presidential authorization was renewed quarterly, but after a December 2005 *New York Times* story about a U.S. government warrantless wiretapping,[7] one telecommunications operator requested that the government file court orders rather than seeking the data under a presidential authorization.[8] The Foreign Intelligence Surveillance Court (FISC) signed the first order placing telephony metadata collection under Foreign Intelligence Surveillance Act authorities in May 2006,[9] relying on the business records provision of the USA PATRIOT Act.[10]

This action, and the interpretation of the business records provision, was not publicly known until the Snowden disclosures (the first leaked document was a 2006 FISC order directed at Verizon[11]). Consternation over the program—public and Congressional—including over the secret interpretation of the business records provision, led to changes that culminated in the passage of the USA Freedom Act (UFA) in 2015.[12]

UFA preserves collection of CDRs but provides a mechanism preventing "bulk" collection that had been objectionable under the interpretation of the business records provision of the PATRIOT Act. Each court application for metadata collection against a target must include a "specific selection term" (SST) that is delimiting in nature. The SST "specifically identifies a person, account, address, or personal device, or any other specific identifier; and … is used to limit, to the greatest extent reasonably practicable, the scope of information sought."[13] Collection is permitted if the government demonstrates to the Court that "(i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required … to such

---

[6] *See* Report on the President's Surveillance Program, Inspector General Offices of the DOD, DOJ, CIA, NSA, ODNI, Annex: A Review of the Department of Justice's Involvement with the President's Surveillance Program, Report No. 2009-0013-A, at 1 (10 Jul., 2009), https://oig.justice.gov/reports/2015/PSP-09-18-15-full.pdf.

[7] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Calls Without Orders*, NEW YORK TIMES (16 Dec., 2015), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html.

[8] Report on the President's Surveillance Program, Office of the Inspector General, National Security Agency, Working Draft, at 39-40 (24 March, 2009), https://www.emptywheel.net/wp-content/uploads/2013/06/090324-Draft-NSA-IG-Report.pdf. *See* Report on the President's Surveillance Program, Inspector General Offices of the DOD, DOJ, CIA, NSA, ODNI, (10 July, 2009), at 54-55.

[9] For further reading see NATIONAL RESEARCH COUNCIL OF THE NATIONAL ACADEMICS, BULK COLLECTION OF SIGNALS INTELLIGENCE: TECHNICAL OPTIONS, p.19-22 (2015).

[10] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56

[11] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (6 Jun., 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[12] Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act, Pub.L. 114-23.

[13] *Id.*, § 201 (b)(4)(A).

investigation [against international terrorism]; and (ii) there is a reasonable, articulable suspicion (RAS) that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor."[14] The act limits collection to two hops and for a period of at most 180 days. Thus UFA is far more protective of privacy than the PATRIOT Act had been.

But UFA was passed at least a decade too late. By 2015, the value of CDRs for telephone communications, including SMS texts, was past. The remainder of my testimony explains how changes in technology and in foreign-terrorist activities against the U.S. have largely eliminated the value of CDRs.

The period 2000-2010 saw a remarkable adoption of mobile communications. The reason is simple: the infrastructure for such communications is far cheaper to install than for landline telephones. In Yemen the number of mobile phone subscriptions went from fewer than 1 in 500 people in 2000 to 47 in 100 in 2010.[15] Nor is Yemen unique. In 2000 the number of mobile subscriptions per 100 people was 0 in Afghanistan, Iraq, and Libya, but by 2010 those numbers had grown to 35 in 100, 55 in 100, and 177 in 100, respectively.[16] With few exceptions the rest of the developing world has seen similarly rapid growth.[17] New communications infrastructure was built in response to the growing demand. With the new technology, the signaling message is picked up along with the call. Thus the missed connection by U.S. intelligence in 2001 was an artifact of an old switching technology, an artifact that is largely no longer a problem even in remote parts of the world. Had contemporary mobile communications infrastructure and technology been in use in 2001, it would have revealed the number of the other end of the communication calling the al-Qaeda safe house in Sana.

The move to cell phones was only one of a series of changes occurring since the attacks of September 11th that largely mooted the value of the CDR program. One cause was the shift in the way foreign terrorists conducted attacks against the domestic U.S.—inspiring rather than closely

---

[14] *Id.*, § 101 (a)(3)(C)(a)(2).

[15] *Mobile Cellular Subscriptions (per 100 people)*, THE WORLD BANK, https://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=YE&veiw=chart. Note that some users may have more than one subscription.

[16] *Id.*

[17] Exceptions include isolated islands, nations where war was taking place, etc. See *supra* note 15.

directing domestic-based actors—also decreased the value of program. Another was the remarkable—and ongoing—revolution in communications technologies meant that everyone, including terrorists, moved from telephone communications to Internet-based ones. The combined effect of these changes has been the reduction in whatever value the Section 215 metadata collection might have had. I discuss each of these changes in turn, beginning with international terrorism.[18]

The CDR program began during al Qaeda's ascendancy. Osama bin Laden's terrorist group altered the way international terrorism was conducted. Instead of in-country attacks, al Qaeda attacked the "far enemy" through attackers tightly directed from a distance. Al Qaeda was organized along the lines of a multinational corporation, with bin Laden as CEO. It was not an organization for freelancers. Attackers were trained at camps in Afghanistan and Pakistan, then sent abroad. There attacks were carefully directed by al Qaeda handlers who remained in frequent communication with those who were to carry them out.

This method of directing terrorism from afar was successful in the late 1990s. But by the 2010s, foreign terrorist threats against the U.S. were changing. The wars in Afghanistan and Iraq, the targeting of al-Qaeda's leadership, and the paring down of the organization's financing channels made it increasingly difficult for al Qaeda's higher echelons to maintain the old corporate structure. Al Qaeda's leaders operated while in hiding and had far less ability to manage the centralized command-and-control structures that had characterized the organization in its heyday.[19]

Al Qaeda was essentially becoming a brand name comprising regional franchises. Ex-CIA operations officer Marc Sageman described this version of al Qaeda as an exporter of a "leaderless jihad"; the terrorist group provided ideology but not organizational structure,[20] while journalist Jason Burke likened al Qaeda to "a venture capital firm—providing funding, contacts, and expert advice to many different militant groups and individuals from all over the Islamic world."[21] Junior

---

[18] A deeper analysis of all of these can be found in Susan Landau and Asaf Lubin, *Examining the Anomalies, Explaining the Value: Should the USA Freedom Act's Metadata Program be Extended?* (forthcoming), which can be found on the authors' websites.

[19] *Al Qaeda in Yemen and Somalia: A Ticking Time Bomb*, A Report to the Committee on Foreign Relations of the United States Senate, p.5 (21 Jan., 2010), https://www.govinfo.gov/content/pkg/CPRT-111SPRT54494/html/CPRT-111SPRT54494.htm.

[20] *See generally* MARC SAGEMAN, LEADERLESS JIHAD: TERROR NETWORKS IN THE TWENTY-FIRST CENTURY (2008).

[21] Jason Burke, *Think Again: Al Qaeda*, FOREIGN POLICY (27 Oct., 2009), https://foreignpolicy.com/2009/10/27/think-again-al-qaeda-4/.

commanders were beginning to operate independently, with the Islamic State (ISIS) being a leading example of this type of activity.[22]

One striking difference between ISIS and its precursor occurred in recruitment. Al Qaeda's model had been to radicalize fighters after their arrival for training. But ISIS needed foreign fighters for capturing territory. With ISIS conquering—and then defending large areas of Iraq and Syria—the terrorist organization's war strategy relied heavily on recruitment. An effective, relatively inexpensive way to accomplish this was through an online propaganda campaign.[23] ISIS used a "media mix of graphic violence and attractive ideals" to attract recruits who then arrived already partially radicalized.[24]

Like al Qaeda, ISIS was interested in attacking the "far enemy," and part of ISIS training enabled recruits to do so. Foreign fighters returning from the front lines mounted terrorist attacks in Brussels,[25] Paris,[26] London,[27] Manchester,[28] Stockholm,[29] Sri Lanka,[30] and elsewhere around the world. The domestic U.S. remained largely immune from attacks conducted by the returning fighters.[31] This was partially an accident of geography—U.S. recruits could not take a simple land trip to reach Iraq and Syria—and partially the proactive stance of the U.S. government, which was

---

[22] *See generally* BRIAN L. STEED, ISIS: AN INTRODUCTION AND GUIDE TO THE ISLAMIC STATE (2016); WALTER LAQUEUR AND CHRISTOPHER WALL, THE FUTURE OF TERRORISM: ISIS, AL-QAEDA, AND THE ALT-RIGHT (2018).

[23] The United Nations Security Council estimated that terrorist groups such as ISIS and Al-Nusrah Front attracted over 30,000 foreign terrorist fighters from over 100 countries. *See* United Nations Security Council, Counter Terrorism Committee, Foreign Terrorist Fighters, https://www.un.org/sc/ctc/focus-areas/foreign-terrorist-fighters/.

[24] T. HAMID AL-BAYATI, A NEW COUNTERTERRORISM STRATEGY: WHY THE WORLD FAILED TO STOP AL QAEDA AND ISIS/ISIL, AND HOW TO DEFEAT TERRORISTS, pp. 110-111 (2017).

[25] Steve Almasy and Shelby Lin Erdman, *Captured Jewish Museum shooting suspect carried weapons, gas mask*, CNN (2 Jun., 2014), https://edition.cnn.com/2014/06/01/world/europe/france-belgium-jewish-shooting..

[26] Patrick J. McDonnell and Alexandra Zavis, *Slain Paris plotter's Europe ties facilitated travel from Syria*, L.A. TIMES (19 Nov., 2015), https://www.latimes.com/world/europe/la-fg-paris-attacks-mastermind-20151119-story.html.

[27] Ian Cobain, *Parsons Green bomb trial: teenager 'trained to kill by Isis'*, THE GUARDIAN (7 Mar., 2018), https://www.theguardian.com/uk-news/2018/mar/07/parsons-green-tube-bombing-ahmed-hassan-on-trial.

[28] Vikram Dodd, Helen Pidd, Kevin Rawlinson, Haroon Siddique and Ewan MacAskill, *At least 22 killed, 59 injured in suicide attack in Manchester arena*, THE GUARDIAN (23 May, 2017)

[29] *Uzbekistan says told West that Stockholm attack suspect was IS recruit*, REUTERS (14 Apr., 2017), https://www.reuters.com/article/us-sweden-attack-uzbekistan/uzbekistan-says-told-west-that-stockholm-attack-suspect-was-is-recruit-idUSKBN17G0J1; *Stockholm truck attack suspect 'interested in Isis': Police*, THE LOCAL (9 Apr., 2017), https://www.thelocal.se/20170409/truck-attack-suspect-rejected-asylum-seeker-interested-in-is-police.

[30] Jason Burke, *Pressure builds on Sri Lankan officials as ISIS claiams Easter attack*, THE GUARDIAN (23 Apr., 2019), https://www.theguardian.com/world/2019/apr/23/pressure-builds-on-sri-lankan-officials-as-isis-claims-easter-attacks.

[31] *See* Alexander Meleagrou-Hitchens, Seamus Hughes and Bennett Clifford, *The Travelers: American Jihadists in Syria and Iraq*, GEORGE WASHINGTON PROGRAM ON EXTREMISM, p.2 (Feb. 2018), https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/TravelersAmericanJihadistsinSyriaandIraq.pdf

the first country in the world to outlaw foreign fighting.[32] Thousands of Europeans joined ISIS, [33] but only 300 Americans are believed to have done so.[34]

Those seeking to return into the United States to carry attacks undergo the scrutiny of both airport security and tight border restrictions. Vetting by U.S. Customs and Border Protection authorities upon entry is one form of protection. Upon entry, domestic law enforcement is very likely to monitor behavior.[35] (Note that such monitoring is unlikely to rely on Section 215 metadata collection. The entry into the United States of a foreign terrorist fighter should constitute sufficient suspicion to justify a traditional FISA warrant.) In examining jihadi plots in the U.S. occurring between 1990 and 2010, Christopher Wright found that those "involving returnees are more prone to detection and therefore disruption."[36] These measures taken against returnees have proven successful.

ISIS has nonetheless been a threat to the domestic U.S. That stems from its ability to wage war through communications. The reason is its online presence and, in particular, its electronic recruitment efforts, which involve not just enrolling foreign fighters but also engaging actors in their home countries to conduct attacks there.

When ISIS was at its height, its social media wing had over 46,000 Twitter accounts; 20% of its followers designated English as their primary language.[37] With online tools to radicalize perpetrators, ISIS encouraged those who stayed at home to carry out attacks there. A mere response or a retweet could be enough for ISIS to focus attention on a specific individual with an eye towards recruitment—but the recruitment would often be in the form of encouraging and inspiring attacks, not directing them. Al Qaeda's *Inspire* magazine once called this method of waging battle "Open Source Jihad."[38] Perpetrators were radicalized online and carried out the attacks alone, or in a small partnership without prior direction and control from ISIS affiliated leaders.

---

[32] *See* 18 U.S. Code § 959, 62 Stat. 745 (2012).

[33] *See* Meleagrou-Hitchens et. al., *supra* note 31, at p.5.

[34] *Id.*

[35] *Id.*

[36] *See* Christopher J. Wright, *How Dangerous Are Domestic Terror Plotters with Foreign Fighter Experience? The Case of Homegrown Jihadis in the US*, 10(1) PERSPECTIVES ON TERRORISM 32, 37 (2016).

[37] *See* Robin Maria Valeri, *From Declarations to Deeds: Terrorist Propaganda and the Spread of Hate and Terrorism Through Cyberspace*, *in* TERRORISM IN AMERICA (Valeri and Brogeson eds., 2018).

[38] For further reading *see* Barry Richards, *Inspire magazine and the rise of open-source jihad*, THE CONVERSATION (19 May, 2013), https://theconversation.com/inspire-magazine-and-the-rise-of-open-source-jihad-14013 Marc Sageman has introduced the concept of a "Leaderless Jihad", which he described as a four-step process through which Muslim youth become radicalized to commit terrorist attacks, most often through "internet-based venues." Sageman, *supra* note, 20.

FBI Director Christopher Wray described the homegrown violent extremists "lack of a direct connection with a foreign terrorist organization" this way:

> In recent years, prolific use of social media by foreign terrorist organizations has greatly increased their ability to disseminate their messages. We have also been confronting a surge in terrorist propaganda and training available via the Internet and social media. Due to online recruitment and indoctrination, foreign terrorist organizations are no longer dependent on finding ways to get terrorist operatives into the United States to recruit and carry out acts of terrorism. Terrorists in ungoverned spaces – both physical and cyber – readily disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause. They motivate these individuals to act at home or encourage them to travel.[39]

Note that this is not the support provided through the tightly scripted attacks organized by al Qaeda; instead, ISIS's tactics consist of radicalization and quite general instructions. The solo attacker, and occasional small group of attackers, commit their action without the prior direction and tight control that had been typical of al Qaeda. That was one radical transformation that has changed the value of the Section 215 metadata collection.

The other was the revolution in communications that has occurred over the last two decades. If the adoption of cellphones completely changed how easily people in remote parts of the world can communicate, an even more notable transformation occurred with smartphones. Laptops have enabled mobile IP communications for decades, but the combination of ease of use and form meant that IP-enabled cellphones—smartphones—have completely transformed how people communicate. As I wrote in 2017, "A … profound change to society began about ten years ago. With cellphones, we made ourselves accessible at any time, from any place. Facebook became publicly available in 2006; the iPhone, in 2007. The combination of social media and a device that you could carry with you proved irresistible."[40] By 2017, "Ninety percent of South Koreans carr[ied] a smartphone, as [did] 77 percent of Australians, 72 percent of Americans, and 58 percent of

---

[39] Christopher Wray, Director of the Federal Bureau of Investigation, Statement Before the Senate Homeland Security and Governmental Affairs Committee, "Threats to the Homeland," p.2 (10 Oct., 2018). https://www.hsgac.senate.gov/imo/media/doc/Testimony-Wray-2018-10-10.pdf.

[40] Susan Landau, LISTENING IN: CYBERSECURITY IN AN INSECURE AGE, 4 (Yale University Press, 2017).

Chinese. The populations of Spain, New Zealand, the United Kingdom, and Canada have embraced smartphones with similar enthusiasm. The revolution took place seemingly overnight. Today, almost all of us carry mobile computers, and we do so almost all the time."[41]

The Internet enables communications in an ever increasing variety of ways. In the Public Switched Telephone Network (PSTN) world of the 1980s, electronic communications were essentially phone calls, faxes, telegrams, and telexes. Today's electronic communications are not only phone calls, SMS, and MMS—the types afforded by the telephone network—they are also email, text messaging apps, chat, Voice over IP, and in-application communications—Internet-based communications. The latter is but a partial list, since innovation proceeds apace for Internet-based communications. Indeed, it is only a modest exaggeration to say that capabilities of such communications are restricted more by an engineer's imagination than by physical limitations.

Not only has the public taken advantage of these rich forms of communications, but so have terrorist organizations. Recall FBI Director Wray's statement about the "lack of a direct connection." The foreign terrorist modus operandi for radicalization is running inciteful videos and texts, attracting followers. The initial presumption of 215, that a selector belonging to specified foreign terrorist organization could be connected to domestic operatives,[42] is not present in the ISIS model of online radicalization and recruitment. It is not present because of the mode of operation of the organizations—broadcasting propaganda via the Internet and then, when there is direct contact, transitioning to IP-based apps.

Two aspects of change are critical here. First, there is no set of telephone communications—by which I mean calls and SMS texts—directly from a terrorist commander to a foot soldier. Instead there is propaganda broadcast via the Internet, and interested parties view the sites.[43] Second, the communications are Internet communications, not PSTN-based. Internet-based applications do not leave the type of CDR records that the Section 215 metadata collection program currently addresses. If we believe that Section 215 metadata collection program is not used for Internet-based communications—an issue I will discuss in a moment—then the Section 215 CDR program does not provide useful information.

---

[41] *Id.*

[42] The FISC must approve the that the selector satisfies the RAS criterion.

[43] The *New York Times* reported that SMS logs are also collected under UFA; *see* Charlie Savage, *Disputed N.S.A. Phone Program Is Shut Down, Aide Says*, N.Y. TIMES (4 Mar., 2019), https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html, which reported on the collection of log data pertaining to texts under CDR authorities; this was then confirmed in an email exchange on March 8, 2019.

ISIS relies heavily on such apps as WhatsApp, Surespot, Viber, Telegram, and Signal.[44] Apps like Telegram, Wickr, and SureSpot are not only end-to-end encrypted; they also provide the ability to send messages that self-destruct and an ability to prevent forwarding of the communication. One particular use of these apps includes spreading propaganda—especially in situations where Twitter accounts have been suspended. Telegram channels allow for mass propagation of news from the caliphate to targeted audiences, which comes in useful when Twitter accounts are subjected to stricter takedown efforts.[45]

Some have argued that UFA could also permit collecting communications metadata from encrypted messaging apps and other Internet communications.[46] I believe that for pragmatic reasons Section 215 authorities are not used in collecting communications metadata of Internet-based communications. Internet-based communications applications are far more complex than PSTN-based ones,[47] and new such applications are constantly being developed.[4849] Applying UFA to Internet-based communications would require specific authorizations around each and every individual new—or newly modified—protocol and app. Obtaining FISC approval for each application is complex and time consuming, involving a heavy use of technical and legal capabilities.

In 2011 the NSA discontinued a program to collect metadata from email communications "for operational and resource reasons." The UFA program is quite stringent—notably more so than the authorities under which the email metadata collection was working in 2011. It seems far more likely that rather than relying on 215, NSA is using Section 702's authorities for the collection of the metadata and content of Internet communications.[50]

The authorities afforded by 702 offer far greater flexibility in addressing these pressing needs; note, though, that targets under 702 cannot include U.S. persons or people located in the US; such individuals can be targets under 215. An analysis of the Intelligence Community (IC)

---

[44] *See* MALCOLM NANCE AND CHRIS SAMPSON, HACKING ISIS: HOW TO DESTROY THE CYBER JIHAD, 176 (2017).

[45] *Id.*, at p.177.

[46] *See* Sharon Bradford Franklin, *Fulfilling the Promise of the USA Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records*, JUST SECURITY (28 Mar., 2019), https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records/.

[47] See, e.g., Steven M. Bellovin, Matt Blaze, Susan Landau, and Stephanie Pell, It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law, 30(1) HARV. J. L. & TEH 1 (2017).

[48] There are multiple reasons for this, including the fact that many IP-based communications applications run within a single platform (e.g., iMessage, WhatsApp, Messenger), and thus can be deployed quickly.

[49] *See* Glenn Greenwald and Spencer Ackerman, *NSA Collected US email records in bulk for more than two years under Obama*, THE GUARDIAN (27 Jun., 2013), https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

[50] This is also the view of independent journalist Marcy Wheeler.

statements and actions about the two programs shows strong language in describing the value of 702. This should not be a surprise to the board. Already in 2014, PCLOB reported that, "[O]ver a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted."[51] It appears that even prior to this year's purge, 215 was used in fewer and fewer cases.

As PCLOB has noted in its 2014 Report, the Section 215 metadata collection program "is not utilized in a vacuum."[52] The global move first to cellular communications and then to mobile IP-based applications, the change in terrorist organizational structure and direction, and the ability to secure communications via IP-based services make Section 215 metadata collection a poor fit for today's investigations of foreign-terrorist attacks directed against the U.S. homeland. The value of the UFA program can only be understood when compared to what capabilities other legal authorities provide to the intelligence community; this includes the signals intelligence that the NSA captures under Section 702, Executive Order 12333, and traditional wiretaps. There are also more traditional FBI techniques that can be used in terrorist investigations.

When the Section 215 metadata collection program was disclosed by Edward Snowden in June 2013, the public's immediate response to the bulk collection program was strongly negative. Congress took notice. Despite testimony of the intelligence community over the value of the bulk metadata collection, in July 2013 bill restricting the collection failed by just twelve votes in the House of Representatives.[53] There was also action on other fronts: ACLU, other civil-liberties organizations, and individuals filed lawsuits challenging the program's legality.[54] The focus was largely on the program's infringement of privacy rights and civil liberties rather than its efficacy.

That focus made some sense. Yet efficacy is basic to any calculus of balance between privacy, civil liberties, and public safety— and questions of efficacy are rooted in pragmatism. Under current circumstances, the CDR collection is not efficacious, and *it is unlikely to be so in future.*

---

[51] Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Privacy and Civil Liberties Oversight Board (PCLOB), 10 (2 Jul., 2014) https://www.pclob.gov/library/702-Report.pdf

[52] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, Privacy and Civil Liberties Oversight Board (PCLOB), at p. 144 (23 Jan., 2014) https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

[53] Spencer Ackerman, *NSA surveillance: narrow defeat for amendment to restrict data collection*, THE GUARDIAN, (25 Jul., 2013), https://www.theguardian.com/world/2013/jul/25/nsa-surveillance-amash-amendment-narrow-defeat.

[54] *See, e.g.*, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y), 959 F.Supp.2d 724 (28 Dec., 2013), https://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf; *Klayman et. al. v. Obama et. al.*, No. 14-5004 (D.C. Cir.), 142 F.Supp.3d 172 (11 Jun., 2013) http://www.freedomwatchusa.org/pdf/130612-PRISM%20Complaint.pdf.

This demolishes the argument for continuing the program. I believe we should do as NSA is said to have recommended and shelve the 215 metadata collection program.[55]

It seems unlikely that in the current situation there will be much enthusiasm for a serious reorganization of surveillance authorities. But PCLOB is in the business of privacy and civil-liberties oversight, not legislative sausage making. PCLOB should recommend the end of the 215 program.

Ending the program should not be confused with allowing all of the FISA provisions subject to sunset. Congress would need to craft an amendment carefully to end only UFA's authorization for collection of CDRs on an ongoing basis. Such an amendment would need to retain safeguards such as UFA's requirement that all Section 501 applications must include a "specific selection term" as the basis for the production. This would allow the government to continue to rely on Section 501 to collect business records without permitting bulk collection. This would enable ending the UFA version of the CDR program, which has been no more effective than the bulk collection program that preceded it. There is no justification in continuing an ineffective program—and all the more so when the program creates a privacy intrusion.

Thank you.

---

[55] *See* Dustin Volz and Warren P. Strobel, *NSA Recommends Dropping Phone Surveillance Program*, WALL STREET JOURNAL (24 Apr., 2019), https://www.wsj.com/articles/nsa-recommends-dropping-phone-surveillance-program-11556138247.