If It Isn't Efficacious, Don't Do It

Susan Landau*

During the 1990s Crypto Wars, in which US export controls on cryptography effectively prevented the use of strong encryption domestically,¹ the Director of the US Federal Bureau of Investigation, Louis Freeh, would often speak publicly about the problems cryptography would pose to using wiretapping in solving kidnapping cases.² But between 1968, when the federal statute providing for wiretapping in such cases became law, and 1993, wiretapping was used in fewer than three cases a year³—even though by the mid 1990s there were approximately 500 kidnappings a year.⁴ Wiretaps were simply not particularly efficacious in kidnapping cases.

When we discuss government surveillance, it is common for the conversation to quickly devolve into a debate about privacy versus security. Yet the data regarding the role of wiretaps in kidnapping cases illustrates the importance of efficacy. The issue of privacy versus security is simply the wrong first question to ask in cases of surveillance programmes. Efficacy should be raised first. If a programme is not efficacious, there is no justification for any intrusion into privacy or civil liberties.

That brings us to the collection of Call Detail Records (CDRs) by the US National Security Agency (NSA) and the question of its efficacy. This was a programme created in response to the attacks of 11 September 2001; it allowed for NSA collection of domestic CDRs in bulk and then permitted NSA analysts to search the collection for CDRs within three 'hops' of a 'selector' believed to belong to a foreign terrorist organisation.⁵ Instituted through presidential authorisation in the hurried days immediately after the 2001 attack, over time the programme shifted to Foreign Intelligence

DOI: 10.21552/edpl/2019/4/4

* Susan Landau is Bridge Professor in Cyber Security and Policy at the Fletcher School of Law & Diplomacy and the School of Engineering, Department of Computer Science, Tufts University, US. This research was supported in part by funding from the William and Flora Hewlett Foundation under grant 2018-7277; any errors are the responsibility of the author. For correspondence: <susan.landau@tufts.edu>.

1 Whitfield Diffie and Susan Landau, 'The Export of Cryptography in the 20th Century and the 21st' in Karl De Leeuw and Jan Bergstra (eds), *The History of Information Security: A Comprehensive Handbook* (Elsevier 2007).

2 Joint Hearings before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary, Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services, Louis Freeh, Director, Federal Bureau of Investigation (18 March 1994), 13 and Hearing before the Senate Committee on the Judiciary, Encryption, Key Recovery, and Privacy Protection in the Information Age, Louis Freeh, Director, Federal Bureau of Investigation (9 July 1997), 39 <<https://www.loc.gov/law/find/hearings/pdf/00140120273.pdf>> accessed 25 November 2019.

3 This was compiled from Table 3 of the 1968-1993 annual reports of the Administrative Office of the United States Courts, *Wiretap Report* (Government Printing Office).

4 In 1995 the FBI reported 624 kidnappings in 1990, 481 in 1991, 495 in 1992, 401 in 1993, and 418 in 1994; letter from Michael Kortan, Unit Chief, FBI National Press Office to author (7 August 1995).

5 A selector could be a phone number, a phone identification number (IMEI), a calling card number etc.

Surveillance Court (FISC) oversight. It was not publicly known until the Snowden disclosures. After the ensuing public debate, a new law, the USA FREEDOM Act (UFA), was passed. Under UFA, the CDR records were stored at the service providers, a situation already occurring for business reasons. NSA access could occur only under a FISC order and only for records within ‘two hops’ of a selector—a phone number, IMEI (phone identification number), calling card number—for which there was reasonable and articulable suspicion that the selector was associated with a foreign power or agent of a foreign power engaged in international terrorism; the new law also required annual reporting on the collection, including the number of CDRs per court order.

At first it appeared that the new law was working well. UFA required annual ‘transparency reports’; the high numbers of CDRs collected for the relatively few targets

Table 1.

Year	Number of Orders	Number of CDRs collected by NSA— fnref:8—
2016	40	151,230,968
2017	40	534,396,285
2018	14	434,238,543

caused concern. A greater cause for concern arose in June 2018 when the NSA announced the deletion of three years’ worth of CDRs collected under UFA. The agency had noticed ‘technical irregularities in some data received from telecommunications service providers’ and decided ‘it was infeasible to identify and isolate properly produced data.’⁶

The USA FREEDOM Act is due to be renewed in December 2019. Understanding the issues as well as the programme's value prior to anticipated renewal in late 2019 was thus quite important. Using public information, a combination of studies on phone usage, knowledge of cellular phone systems, and basic arithmetic, I concluded that the high numbers appeared to be due to high-volume callers⁷ and that the technical irregularities were likely due to the complexities of the CDRs for roaming cellphones.

I also studied efficacy. In 2014 the Privacy and Civil Liberties Oversight Board (PCLOB), having concluded in 2014 that the bulk metadata had been useful in identifying only one previously unknown suspect in the US, had also raised issues of efficacy.⁸ Of

⁶ *ibid.*

⁷ *ibid.* 30.

⁸ Privacy and Civil Liberties Oversight Board, ‘Report on the Telephone Records Programme Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court’ (23 January 2014), 152-153 (‘PCLOB report’).

course, the programme provided other value beside identifying suspects. It helped in triaging, enabling investigators to eliminate false suspects, and it enabled investigators to go ‘backwards in time’ and collect alternate identifiers for suspects who were only identified later.⁹

That was in 2014, but this was 2019. Many aspects of this collection, including technology and terrorist threats, had changed between the time of the programme’s origin in 2001 and the present. During the heyday of al Qaeda in the late 1990s and early 2000s, the modus operandi for conducting terrorist attacks against the ‘far enemy’ (the US and the West) was directing cells within those nations. The cell’s actions were carefully managed by the overseas operatives. By the early 2010s, the central leadership of al Qaeda had been badly damaged, and a new model for directing terrorism at the US was emerging. Foreign-based recruiters would incite potential recruits within the US over the Internet, then switch to encrypted communications to provide further encouragement.

When ISIS declared the caliphate in 2014, it sought foreign fighters to bolster its ranks. ISIS operated a sophisticated online presence through Twitter—in 2014 it had 46,000 accounts¹⁰—and Internet videos. Once a potential recruit expressed interest in ISIS, the conversation would shift to secure Internet communications applications such as WhatsApp, Surespot, Viber, Telegram, and Signal.¹¹

These efforts were effective in obtaining recruits from Europe; tens of thousands of Europeans went to Iraq and Syria to join ISIS.¹² ISIS was much less successful in drawing volunteers from the US (it is believed only about 300 Americans joined ISIS¹³). When someone in the US responded to an ISIS online effort, the communication moved to encrypted applications, the intent, not recruitment but instead encouraging an attack within the US. This model became the modern foreign-inspired domestic terrorist threat. By 2018 FBI Director Christopher Wray saw, ‘[H]omegrown violent extremists [as] the greatest terrorism threat to the homeland. These individuals ... who are in the US, have been radicalized primarily in the US’¹⁴

9 Committee on Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals Intelligence Collection, Bulk Collection of Signals Intelligence: Technical Options 9 (National Research Council of the National Academies, 2015), 9.

10 Robin Maria Valeri, ‘From Declarations to Deeds: Terrorist Propaganda and the Spread of Hate and Terrorism Through Cyberspace’ in Robin Maria Valeri and Kevin Brogenson (eds), *Terrorism in America* (Routledge 2018).

11 Malcolm Nance and Chris Sampson, *Hacking ISIS: How to Destroy the Cyber Jihad* (Skyhorse 2017), 176.

12 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/>> accessed 21 August 2019. The majority of these were from Europe. As of 2016, it was estimated that 700 Southeast Asians were recruited by ISIS to fight in Iraq and Syria; most were from Indonesia; see Testimony of Joseph Chinyong Low, Senior Fellow, Foreign Policy, Center for East Asia Policy Studies, The Brookings Institution, in Hearing before the House of Representatives, Committee on Homeland Security (27 April 2017) ISIS in the Pacific: Assessing Terrorism in Southeast Asia and the Threat to the Homeland.

13 Alexander Meleagrou-Hitchens, Seamus Hughes and Bennett Clifford, ‘The Travelers: American Jihadists in Syria and Iraq’ (The George Washington University, February 2018), 5 <<https://extremism.gwu.edu/sites/g/files/zaxdzs2191/f/TravelersAmericanJihadistsinSyriaandIraq.pdf>> accessed 21 August 2019.

14 Christopher Wray, Director of the Federal Bureau of Investigation, Statement Before the Senate Homeland Security and Governmental Affairs Committee, ‘Threats to the Homeland’ (10 October 2018), 2.

These US terrorists were ‘lone wolves,’ acting individually. ISIS operatives didn’t direct attacks but provided general encouragement.¹⁵ Wray described the shift as a ‘significant transformation’ from the terrorist threat of a decade earlier.¹⁶

This changed investigative techniques. These foreign-inspired domestic terrorists were neither closely directed by foreign terrorists nor were they using the telephone to plot. Authorities provided by Section 702 of the FISA Amendments Act, which permits warrantless collection against non-US persons located outside the US¹⁷—thus making their communications and data stored at US providers such as Google, Facebook, Microsoft, etc accessible to US investigators—was becoming increasingly valuable; CDRs were much less valuable than they once had been (and, as PCLOB noted, even in the 2000s there was ‘little evidence that the unique capabilities provided ... by the bulk collection ... actually have yielded ... results ... that could not have been achieved without ... the program’¹⁸).

Comments from the Intelligence Community reflected this shift. In May 2012, the Director of Legislative Affairs at the Office of Director of National Intelligence (ODNI) and a Department of Justice Assistant Attorney General wrote the Senate Select Committee on Intelligence that the Section 702 powers were critical in the ‘Government’s efforts to acquire foreign intelligence necessary to protect the nation’s security.’¹⁹ In February 2016, Intelligence Community leadership described the 702 programme as providing ‘critical foreign intelligence that cannot practicably be obtained through other methods.’²⁰ In 2017, NSA General Counsel Glenn Gerstell said that ‘Section 702 represents one of NSA’s most important intelligence surveillance authorities, and it provides tremendous value in the nation’s fight against foreign terrorists.’²¹

This makes sense. While not all social media and cloud platforms are US based, many are. Not only are Section 702 authorities valuable now; they are expected to be for quite some time.

By contrast, even as the USA FREEDOM Act was passed in 2015, the language describing the value of the CDR collection was quite muted. When the programme was discussed, it was in the context of various surveillance tools. Often discussion of the

15 *ibid.*

16 *ibid.*

17 This is the FISA Amendments Act of 2008 (15 USC 1881 (a)).

18 PCLOB report (n 10) 146.

19 Letter from Kathleen Turner, Director of Legislative Affairs, Office of the Director of National Intelligence, and Ronald Weich, Assistant Attorney General, Office of Legislative Affairs, DOJ to Senator Dianne Feinstein and Senator Saxby Chambers of the Select Committee on Intelligence (4 May 2012).

20 Unclassified Joint statement of Robert S. Litt, Gen. Counsel of the Office of the Dir. of National Intelligence, Stuart J. Evans, Dep. Asst. Attorney General for Intelligence, US Dept. of Justice, Michael B. Steinbach, Ass. Dir. Counterterrorism Div., Federal Bureau of Investigation & Jon Darby, Chief of Analysis and Production, Signals Intelligence Directorate, National Security Agency, Briefing on the FISA Amendments Act Before the S. Comm. on the Judiciary, 114 Cong. 9 (2 February 2016), 9.

21 Glenn S. Gerstell, *Judicial Oversight of Section 702 of the Foreign Intelligence Surveillance*, Lecture to the Robert S. Strauss Center for International Security and Law and The University of Texas School of Law, Austin, Texas (14 September 2017).

value of the CDR programme would be combined with discussion of other uses, as in the ‘bulk collection programmes.’²² In defending CDR NSA Director Alexander argued that the combination of programmes ‘contributed to our understanding, and in many cases helped enable the disruption of terrorist plots.’²³

Even two years before the passage of the USA FREEDOM Act (UFA), the use of CDRs was not particularly efficacious. Given this, there is a question of why pass UFA? And now history is repeating: even as the NSA purged three years’ of CDRs and has halted the programme indefinitely, the White House is seeking the law’s reauthorisation.²⁴ Asking the efficacy question—which is the first issue legislators should consider—would give a resounding ‘no’ to continuing the authorities provided by the law.

Efficacy should always come first. Asking the efficacy question requires looking hard at the value of a programme. What does it produce? Is the production worth it? Are there alternate ways of learning needed information that are less costly? What’s the opportunity cost, that is, what resources—people, funds, expertise, engineering—are being used here that could be more effectively be spent elsewhere? Personnel and budgets are not infinite; asking these hard questions causes those deploying the tools to carefully focus on utility.

Only when the question is answered—positively—should the issues of the threat to privacy and civil liberties become part of the discussion. This does not mean that questions of privacy and civil liberties are not critically important in determining whether to use particular surveillance or security tools. They are, and we must never lose the moral compass they provide. But as I said earlier in this foreword, if a programme is not efficacious, there is no justification for any intrusion into privacy or civil liberties. Indeed, if a programme is not efficacious, there is no need to consider it further.

22 See, eg, Testimony of General Keith Alexander, Hearing of the House Permanent Select Committee on Intelligence on How Disclosed NSA Programmes Protect Americans, and why Disclosure Aids our Adversaries (18 June 2013).

23 Gen. Keith Alexander, Commander, US Cyber Command (USCYBERCOM), Director, National Security Agency (NSA), Chief, Central Security Service (CSS) at AFCEA International Cyber Symposium (28 June 2013).

24 Charlie Savage, ‘Trump Administration Asks Congress to Reauthorize N.S.A.’s Deactivated Call Records Programme’ *NY Times* (15 August 2019).