PART III - SURVEILLANCE, OVERSIGHT, SKEPTICISM, AND RACE

Lessons for the Next Twenty Years: What the Two Decades Since 9/11 Have Taught Us About the Future of Foreign Intelligence Surveillance Law

David S. Kris*

This document was reviewed for classified information by the U.S. government.

INTRODUCTION

I am tempted to begin this essay with well-known quotations from Edmund Burke[1] and Yogi Berra.[2] Their advice, which I will follow, is to study the past seriously but predict the future with humility and a sense of humor. I have written elsewhere about forthcoming technical issues in the field of foreign intelligence surveillance law, but this essay considers more generally how surveillance law evolves.[3] It examines five major developments and identifies five major lessons.

* David S. Kris is a founder of Culper Partners, LLC.

1. *"Those who don't know history are doomed to repeat it,"* Quotation by Edmund Burke, KNOWYOURQUOTES, https://perma.cc/4A28-QUA9.

2. *"It's tough to make predictions, especially about the future,"* Quotation by Yogi Berra, GOODREADS, https://perma.cc/36KM-FHD7.

3. David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance,* HOOVER INST. (2016), https://perma.cc/3FPL-PPVN; David S. Kris, *Digital Divergence,* NAT'L CONST. CTR., https://perma.cc/VFA8-Z4MF; David S. Kris, *FISA Reform Opinion by David Kris* (August 2020), https://perma.cc/SW58-NG7F.

I. DEVELOPMENTS IN FOREIGN INTELLIGENCE SURVEILLANCE LAW

The last half-century has witnessed five major developments in foreign intelligence surveillance law: (1) enactment of the Foreign Intelligence Surveillance Act (FISA) in 1978; (2) the demise of the FISA Wall in 2002; (3) FISA modernization culminating in 2008; (4) bulk metadata collection as revealed in 2013; and (5) FISA accuracy reforms highlighted most recently in 2020. These five developments have been shaped by a system of separated powers, challenged by the competing needs for secrecy and democratic legitimacy, affected unpredictably by unauthorized disclosures, and stressed periodically by policy and political preferences.

A. The Foreign Intelligence Surveillance Act (1978)

In my lifetime, there have been two major moments of political consensus concerning surveillance law. The first occurred in the mid-1970s, when the Church Committee and others revealed massive and horrific abuses by the U.S. Intelligence Community and galvanized opinion in favor of new limits on government.[4] (The other moment of consensus, immediately after the 9/11 attacks, is discussed below.) In this period, only the most stalwart guardians of Article II resisted retrenchment – and more than 20 years later, with the paradigm of intelligence under law and the doctrine of separation of powers both more clearly established, there was room for some self-deprecating humor that I think Yogi Berra would have approved.[5]

In this period, secrecy yielded to public disclosure on many fronts, given the extreme nature of the abuse revealed, but several known-unknown areas remained, including with respect to electronic surveillance conducted abroad. Testifying before Congress in 1976, for example, Attorney General Ed Levi summarized testimony given in a prior closed hearing by the Director of the NSA, General Lew Allen, describing "an awesome technology – a huge vacuum cleaner of communications – that had the potential for abuses."[6] When it enacted FISA, Congress explicitly declined to regulate such electronic surveillance, noting "with approval" that the executive branch had adopted limits on it in the predecessor to Executive Order 12333.[7] Self-imposed restrictions also reduced the pressure to enact legislative charters for intelligence agencies.[8] Congress did, however, assert itself by creating the intelligence oversight committees, and at various times enacting legislation requiring the executive branch to keep them "fully and currently informed."[9]

4. CHURCH COMMITTEE REPORTS, AARC Public Library Contents, https://perma.cc/NY57-F3X3.

5. *See In re Sealed Case*, 310 F.3d 717, 732 n.19 (FISA Ct. Rev. 2002).

6. *See* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 16:5 at 601 (3d ed. 2019) [hereinafter NSIP].

7. *Id.* § 17:1 at 654.

8. *Id.* §§ 1:4 at 12, 2:7 at 50, 16:5 at 609-10.

9. *Id.* § 2:7 at 63-64.

B. The FISA Wall (2002)

The September 11 attacks produced a second major moment of U.S. political consensus on surveillance and related issues of national security: the USA Patriot Act, which expanded governmental authority, passed in the Senate by a vote of 98-1.[10] Perhaps the most significant change to emerge from this consensus, at least with respect to surveillance law, was the lowering of the so-called FISA "Wall" that limited interaction between intelligence and law enforcement officials. This change involved all three branches of government working in concert, with Congress enacting two relevant provisions (Sections 218 and 504 of the Patriot Act), the Justice Department adopting new procedures to implement those provisions, and the FISA Court of Review upholding those procedures and the constitutionality of the statute in a published opinion after litigation involving *amici curiae* who filed briefs opposing the government.[11] Since then, both provisions of law have remained in force, with one of them having been renewed by Congress against the background of the Court of Review's decision. I have argued that lowering the FISA Wall was an enhancement of both security and civil liberties rather than a zero-sum reallocation between them.[12]

C. FISA Modernization (2008)

The consensus of 9/11 did not last long. In the immediate aftermath of the attacks, George W. Bush authorized the President's Surveillance Program (PSP), one element of which was the Terrorist Surveillance Program (TSP), a collection program that acquired the contents of messages with one end in the United States.[13] This was done in secret, with limited notification to the congressional intelligence committees and to the FISA Court. The *New York Times* revealed the surveillance in December 2005, which triggered a political firestorm: this was the very opposite of consensus, with divisions along political party lines focused on whether and how to emphasize speed and agility in counterterrorism as opposed to privacy and civil liberties. In January 2007, at the urging of the Department of Justice in a classified, *ex parte* proceeding, the FISA Court initially authorized but then declined to reauthorize a program of surveillance that resembled the TSP.[14] At that point, the executive branch engaged with Congress, securing passage of the Protect America Act (PAA) in 2007 and, when that law proved to be technically deficient, the FISA Amendments Act in 2008 (FAA), which has

10. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT), Pub. L. No. 107-56, 115 Stat. 272 (2001).

11. *See In re Sealed Case*, 310 F.3d 717, 732 n.19 (FISA Ct. Rev. 2002); NSIP, *supra* note 6, chapters 10-11.

12. David S. Kris, *The Rise and Fall of the FISA Wall*, 17 Stan. L. & Policy Rev. 487, 523-24 (2006)

13. *The Department of Justice Releases Inspectors General Reports Concerning Collection Activities Authorized by President George W. Bush After the Attacks of September 11, 2001*, INTEL https://perma.cc/28BE-MXV9.

14. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1144 (2013).

endured and was renewed most recently in 2018.[15] The chronology of this period is recounted in detail NSIP §§ 16:7-16:16 (pages 622-645), but for present purposes it makes an interesting contrast with the process of lowering the FISA Wall. Modernization was accomplished not by all three branches of the government acting in concert and more or less in the open, but by the executive branch first proceeding on its own in secret, then – following a media leak – in secret with the judicial branch, and then finally with Congress. The need to replace the PAA with the FAA also shows how complex and difficult the law of surveillance can be.

D. Bulk Metadata Collection (2013)

Like the TSP, bulk collection of telephony metadata and email (digital) metadata commenced in secret as part of the PSP shortly after the 9/11 attacks. Also like the TSP, it was made public by unauthorized disclosures – this time, by Edward Snowden in 2013. Unlike the TSP, however, the two bulk metadata programs were approved multiple times by the FISA Court and fully briefed to Congress. The Congressional Intelligence Committees, in particular, promptly and forthrightly acknowledged having been fully and currently informed. Nonetheless, despite all three branches of government having supported bulk metadata collection, the disclosures ignited another political firestorm (it is difficult to imagine what would have happened if the executive branch had not properly engaged with the FISA Court and Congress). As with the TSP, the result of public disclosure was legislation. Where the FAA was essentially a statutory authorization for the TSP, however, the USA Freedom Act of 2015 restricted bulk metadata collection.[16] By 2013-2015, the 9/11 attacks had receded in importance and American politics were in flux, with elements of the Republican Party becoming more skeptical of surveillance, scrambling prior alignments. The Freedom Act forbade bulk collection under FISA (and through National Security Letters) and substituted a legally and technologically complex program for the ongoing production of call detail records (CDRs). In the end, the CDR program did not function as designed, resulting in NSA purging all of the data collected under the program and discontinuing collection – another lesson in the complexity of the field. Statutory authority for ongoing CDR collection sunset in March 2020 and is very unlikely to be revived, but bulk collection remains available outside of FISA in certain categories specified in PPD-28, a directive issued by President Obama that remains in effect.[17]

15. Protect America Act of 2007, Pub. L 100-55, 121 Stat. 552 (2007); FISA Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (2008).

16. USA Freedom Act of 2015, Pub. L. 114-23, 129 Stat. 268 (2015).

17. Presidential Policy Directive-Signals Intelligence Activities (Jan. 17, 2014); *see* NSIP, *supra* note 6, chapters 18-19.

E. FISA Accuracy (2020)

The final development to be considered concerns the factual accuracy and completeness of FISA applications. Here I should note that our former president and certain of his followers were not pleased with my appointment as *amicus curiae* to help the FISA Court deal with certain accuracy issues in 2020. The President tweeted his disapproval ("You can't make this up! David Kris, a highly controversial former DOJ official, was just appointed by the FISA Court to oversee reforms to the FBI's surveillance procedures. Zero credibility. THE SWAMP!"), and his followers then conveyed their views, often in quite graphic terms, albeit apparently without having read my published work on the issues.[18] Whatever else it reveals, I believe this little episode shows that Yogi Berra was right – no one during or before the Presidency of George W. Bush could have predicted how much would change by 2020!

In any event, FISA accuracy has been a recurring and major issue on at least three occasions, the first of which preceded the 9/11 attacks. In 2000, when the FISA Wall was up and the Court was very concerned about interactions between intelligence and law enforcement officials, the government made a series of significant false statements in applications. As the Court later put it in a published opinion:

> Beginning in March 2000, the government notified the Court that there had been disseminations of FISA information to criminal squads in the FBI's New York field office, and to the U.S. Attorney's Office for the Southern District of New York, without the required authorization of the Court as the 'wall' in four or five FISA cases.[19]

Six months later, in "September 2000, the government came forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States."[20] This second tranche of errors included misstatements and omissions of material facts concerning whether a FISA target was under criminal investigation, separation of parallel intelligence and criminal investigations, and a prior relationship between the FBI and a FISA target. And within another six months,

> the government reported similar-misstatements in another series of FISA applications in which there was supposedly a 'wall' between separate intelligence and criminal squads in FBI field offices to screen FISA intercepts, when

18. *See* David Kris, *Further Thoughts on the Crossfire Hurricane Report,* LAWFARE BLOG (Dec. 23, 2019, 4:19 PM), https://perma.cc/9J3A-WTQ6; Letter Brief of Amicus Curiae David Kris, *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, No. Misc. 19-02 (FISA Ct. Jan. 15, 2020), https://perma.cc/Q35Q-5LC5.

19. *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620 (FISA Ct. 2002).

20. *Id.*

> in fact all of the FBI agents were on the same squad and all of the screening was done by the one supervisor overseeing both investigations.[21]

In response, the FBI developed procedures for verifying the accuracy of FISA applications, known commonly as the "Woods Procedures," which, for a time, worked very well.

A second series of accuracy problems emerged beginning in 2009, this time in FISA applications filed by the NSA, many of them concerning the bulk collection of metadata. These errors are too many, varied, technical, and (in some cases) classified to be summarized conveniently here, but their overall significance is shown by a pointed footnote in a 2011 FISA Court opinion that was later made public:

> The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.
>
> In March, 2009, the Court concluded that its authorization of NSA's bulk acquisition of telephone call detail records from [redacted] in the so-called "big business records" matter "ha[d] been premised on a flawed description of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." . . . Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying. The Court concluded that this requirement had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively."[22]

The third and most recent series of problems, in the FBI's Crossfire Hurricane investigation and FISA applications on Carter Page, revealed deficits in procedures and processes, but also evinced a cultural slippage. Like the accuracy problems of the past, they provoked a strong response from the FISA Court:

> The frequency and seriousness of these errors in a case that, given its sensitive nature, had an unusually high level of review both at DOJ and the Federal Bureau of Investigation have called into question the reliability of information proffered in other FBI applications.[23]

---

21. *Id.* at 621.

22. [REDACTED NAME], [REDACTED NO.], slip op. at 28 (FISA Ct. Oct. 3, 2011) (opinion of Judge John D. Bates), https://perma.cc/DEP3-8XD8.

23. Corrected Opinion and Order, *In re Accuracy Concerns Regarding FBI Matters Submitted to the FISC*, No. Misc. 19-02 at *1 (FISA Ct. Mar. 5, 2020).

One FBI lawyer pleaded guilty to a crime in connection with the applications – an unprecedented event.[24] Work to restore the integrity of FBI FISAs, and the confidence of the Court and the American people, remains ongoing.

II. LESSONS LEARNED

Taking these five developments together – as a series of inflection points in foreign intelligence surveillance law – what do they show us about the past, and what can they tell us about the future? I will highlight five points, among several that might be drawn.

First, foreign intelligence, and national security more generally, are not solely controlled by the President. The Supreme Court has described the President as the "sole organ" of the nation in foreign affairs,[25] but as a practical matter the judicial branch, the legislative branch, private communications providers, the news media and individual leakers all have exerted profound effects on surveillance law and practice in the last half-century. Inter-branch consensus, and public-private partnerships, are always powerful and sometimes essential.

Second, when a moment of political consensus does arrive, huge change is possible. The advent of intelligence under law in the mid-1970s, and the pro-surveillance reforms after 9/11, were profound. There is, however, often a significant tension between acting fast and building consensus. I described above how the FISA Wall was dismantled by all three branches of government working in parallel, while FISA modernization involved them working more in series. But President Bush's TSP was operational within several days of the 9/11 attacks, while the FISA Wall did not come down until November 2002. Both changes have endured: the TSP was controversial when revealed but ultimately enabled by the PAA and the FAA, and the FAA and the Wall-related amendments have survived multiple sunsets. But the other revealed elements of the PSP, involving bulk collection, led to legislation (the Freedom Act) forbidding them.[26] Among other factors, that difference reflects in part the timing of the unauthorized disclosures – 2005 vs. 2013 – and in part the perceived operational value of the different surveillance programs.

Third, however, consensus usually remains elusive. Polarization is more often the rule in American politics, with the added complexity that polarity can change unexpectedly. The Republican Party, in particular, has evolved dramatically since 2008, in its views on surveillance (and in other ways). I am firmly with Mr. Berra on the question of whether and how domestic and international terrorism, including state-sponsored terrorism, will converge: in the late 1990s, when I was prosecuting the Montana Freemen, I would not have predicted links between the

24. Katelyn Polantz, *Judge accepts FBI lawyer's guilty plea for false statement in Carter Page warrant paperwork*, CNN (Aug. 19, 2020, 2:01 PM), https://perma.cc/KPH8-UE8B.

25. *See United States v. Curtiss-Wright Export Corp.*, 299 U.S. 304, 319 (1936).

26. *See* Pub. L. No. 114-23 (2015).

Boogaloo Bois and Hamas,[27] and I do not know what will follow from efforts by the Russian Imperial Movement[28] and other foreign groups to export white supremacy.

In other words, our approach to surveillance law, like our approach to national security generally, depends on political and cultural factors. Viewed from a sufficient distance, at least, surveillance law has roughly tracked the nation's preferences. It will likely continue to do so. As such, absent a galvanizing exogenous event at or above the level of 9/11 or the disclosures of the mid-1970s, our approach in the next few years is likely to reflect division more than consensus, and truly epic change is unlikely.

Fourth, there is an ongoing and worsening political tension posed by secret intelligence operations in a democracy. Both the FAA and the Freedom Act arose from unauthorized disclosures.[29] In the former case, even relevant governmental institutions were kept substantially in the dark; in the latter, judicial and legislative oversight of the intelligence community functioned precisely as it was designed to function, but the result was nonetheless unsatisfactory to the American people. The restrictions of the Freedom Act pretty clearly emerged despite, not because of, proper oversight. As noted above, it is difficult to overstate how bad things would have been with bulk collection if oversight had not been done correctly. But proper oversight and inter-branch consensus is not a guarantee of political support – at least not a durable one.

Today, there are real and perhaps growing challenges with oversight of the Intelligence Community by Congress. As I have written elsewhere, intelligence oversight in this country "has evolved from essentially nothing (1947-1976), to secret proxy oversight through elite members of Congress (1976-2013), to something closer to ordinary political accountability (2013 to present)."[30] Combined with a recent tendency to reject traditional norms of governance, the results have been serious and enduring shortcomings, particularly in the House Permanent Select Committee on Intelligence, most prominently in connection with FISA accuracy issues as discussed above. Without reasonably apolitical and honest oversight, a key element of intelligence under law is in jeopardy. As Courtney Elwood explained in a recent talk at the Council on Foreign Relations, technological change and the growing scope and scale of the intelligence enterprise have also contributed to oversight challenges. In government, as in business, compliance mechanisms tend to lag behind operations: our counter-terrorism adversaries did not attempt seriously to influence elections or divide us politically, and so the

27. *See* Matthew Kriner & Jon Lewis, *The Evolution of the Boogaloo Movement*, 14 CTC SENTINEL 22 (Feb. 2021).

28. *See* Nathan A. Sales, Coordinator for Counterterrorism, Remarks on Designation of the Russian Imperial Movement (April 6, 2020), https://perma.cc/ZW8B-EPAV.

29. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://perma.cc/VD9V-ACBN; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), https://perma.cc/CU5D-5QNP.

30. David Kris, *Analytic Superiority, Public-Private Cooperation and the Future of US Foreign Intelligence*, LAWFARE BLOG (May 17, 2019, 10:18 AM), https://perma.cc/Q9TB-63WS.

checks and balances imposed after 9/11 must adapt as the intelligence community itself adapts to changing technologies and threats.

The fifth and final point is the only real prediction I will venture here, and limited to the relatively near term: evolving technologies and threats, including digital networks and nation-state adversaries with equal or superior capacities to operate within those networks, will leave their mark. One very significant, current challenge relevant to surveillance involves foreign use of domestic infrastructure to attack and steal information.[31] It might be addressed in the near term by a combination of more dynamic approaches to defining FISA "facilities,"[32] better reporting from domestic providers of infrastructure (and other products and services),[33] and perhaps other public-private partnerships. More broadly, the Chinese and others clearly believe that their system of government is superior to ours – in general, and certainly in the cyber age. A net assessment gives them relative advantages in public-private partnerships and unity of action. Our advantages may lie in living up to our traditions of freedom of thought and of opportunity, enabled by rule of law. If we can, I think that is probably how we will prevail in respect of foreign intelligence surveillance and also in most of our other important endeavors.

31. Gen. Paul M. Nakasone, Posture Statement before the 117th Congress (Mar. 25, 2021), https://perma.cc/8PVP-42KY.

32. *See In re Sealed Opinion*, No. 19-218 (FISA Ct. Mar. 5, 2020).

33. *See* Exec. Order No. 13,984, 86 Fed. Reg. 6837 (Jan. 25, 2021).

***