Harvard Journal of Law & Technology
Volume 28, Number 1 Fall 2014

YOUR SECRET STINGRAY'S NO SECRET ANYMORE: THE VANISHING GOVERNMENT MONOPOLY OVER CELL PHONE SURVEILLANCE AND ITS IMPACT ON NATIONAL SECURITY AND CONSUMER PRIVACY

*Stephanie K. Pell & Christopher Soghoian**

TABLE OF CONTENTS

---

* Pell is an Assistant Professor & Cyber Ethics Fellow at West Point's Army Cyber Institute and an Affiliate Scholar at Stanford's Center for Internet & Society. She is a former Counsel to the House Judiciary Committee and has held several positions in the Department of Justice, including Senior Counsel to the Deputy Attorney General and Assistant U.S. Attorney in the Southern District of Florida.

Soghoian is the Principal Technologist with the Speech, Privacy, and Technology Project at the American Civil Liberties Union and a Visiting Fellow with the Information Society Project at Yale Law School. The opinions expressed in this Article are the authors' alone and do not reflect the official position of their respective employers or any part of the United States Government.

The authors wish to thank Matt Blaze, Ian Brown, Alan Butler, Susan Freiwald, Allan Friedman, Jean-Pierre Hubaux, Eric King, Susan Landau, Linda Lye, Aaron K. Martin, Valtteri Niemi, Karsten Nohl, Brian Owsley, Christopher Parsons, Christopher Prince, John Scott-Railton, Greg Rose, Seth Schoen, Jennifer Valentino-DeVries, David Wagner, Nicholas Weaver, several individuals who have asked to remain anonymous, and the attendees of their session at the 2013 Privacy Law Scholars Conference.

I. INTRODUCTION

> ". . . [T]HOU WILT NOT TRUST THE AIR WITH SECRETS." — SHAKESPEARE, TITUS ANDRONICUS[1]

During a 1993 congressional oversight hearing on the integrity of telephone networks,[2] security researcher Tsutomu Shimomura used a "software hack" to turn an analog cellular phone into a scanner that enabled all present in the hearing room to hear the live conversations of nearby cellular phone users.[3] Shimomura had been granted immunity to perform this demonstration under the watchful gaze of a nearby

1. WILLIAM SHAKESPEARE, TITUS ANDRONICUS, act 4, sc. 2.

2. *Telecommunications Network Security: Hearing Before the Subcomm. on Telecomms. & Fin. of the H. Comm. on Energy & Commerce*, 103d Cong. 1 (1993) [hereinafter *Telecommunications Network Security Hearing*] (statement of Rep. Markey, Chairman, Subcomm. on Telecomms. & Fin. of the H. Comm. on Energy & Commerce).

3. *Id.* at 8–9.

agent from the Federal Bureau of Investigation ("FBI").[4] The event was a practical demonstration of what Subcommittee Chairman Ed Markey called "the sinister side of cyberspace."[5]

The demonstration illustrated a significant security vulnerability impacting then-widely used analog cellular phone networks: calls were not encrypted as they were transmitted over the air and could, therefore, be intercepted with readily available equipment,[6] such as an off-the-shelf radio scanner or a modified cellular phone.

Although the threat demonstrated by Shimomura was clear, Congress and the Federal Communications Commission ("FCC") took no steps to mandate improvements in the security of analog cellular calls.[7] Such a technical fix would have required wireless carriers to upgrade their networks to support more secure telephone technology, likely at significant cost.[8] Instead, Congress outlawed the sale of new radio scanners capable of intercepting cellular signals and forced scanner manufacturers to add features to their products to prevent them from being tuned to frequencies used by analog cell phones.[9]

---

4. *See Immunity Needed*; *Markey Panel Sees Dark Side of Electronic Frontier*, COMM. DAILY (Apr. 30, 1993), *available at* https://w2.eff.org/Privacy/Newin/Cypherpunks/930430.communications.daily.

5. *Telecommunications Network Security Hearing*, *supra* note 2, at 1 (statement of Rep. Markey, Chairman, Subcomm. on Telecomms. & Fin. of the H. Comm. on Energy & Commerce).

6. *See* Simson L. Garfinkel, *Understanding Cellular Telephone Security and Privacy*, SIMSON.NET (2007), http://simson.net/ref/security_cellphones.htm ("[Analog cell phones] were the first cellular telephones. Developed in the 1970s and deployed in the 1980s . . . . [t]hese phones transmit voice as an analog signal without any encryption of scrambling.").

7. *See Telecommunications Network Security Hearing*, *supra* note 2, at 9 (statement of Rep. Markey, Chairman, Subcomm. on Telecomms. & Fin. of the H. Comm. on Energy & Commerce) ("[L]ast year we passed legislation to ban scanners, but we clearly did not ban cellular phones. However, cellular phones can be reprogrammed as a scanner with a relatively rudimentary knowledge of the technology. Tens of thousands of people know how to do it."). In a submission to the FCC, the cellular industry association opposed proposals for the FCC to focus on the cellular interception vulnerabilities rather than the availability of radio scanners capable of intercepting cellular phone calls. *See* FED. COMMC'NS COMM'N, REPLY COMMENTS OF THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION ON AMENDMENT OF PARTS 2 AND 15 TO PROHIBIT MARKETING OF RADIO SCANNERS CAPABLE OF INTERCEPTING CELLULAR TELEPHONE CONVERSATIONS 4 (1993) [hereinafter CTIA REPLY COMMENTS], *available at* http://apps.fcc.gov/ecfs/document/view;jsesionid=fTGkSn3c0CsJjGhv2ts5DQQktvyhfXkHpW2JPnr9pPhxQ9sC88Cp!-1864380355!1357496456?id=1120040001 ("Rather than proposing to strengthen the Commission's proposed rules, however, these parties would have the Commission weaken or abandon its proposals and place the [privacy] burden solely on cellular carriers or manufacturers . . . . With the enactment of Section 403(a), the time for such an argument is past.").

8. *See* Craig Timberg & Ashkan Soltani, *By Cracking Cellphone Code, NSA Has Ability To Decode Private Conversations*, WASH. POST (Dec. 13, 2013), http://www.washingtonpost.com/business/technology/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html ("Upgrading an entire network to better encryption provides substantially more privacy for users . . . . But upgrading entire networks is an expensive, time-consuming undertaking . . . ."); Babbage, *infra* note 271. Such network upgrades would also have neutralized analog interception devices, which were then used by U.S. government agencies.

9. *See* FED. COMMC'NS COMM'N, REP. & ORD. FCC 93-201, AMENDMENT OF PARTS 2 AND 15 TO PROHIBIT MARKETING OF RADIO SCANNERS CAPABLE OF INTERCEPTING

This action by Congress, however, did nothing to prevent the potential use of millions of existing interception-capable radio scanners already in the homes and offices of Americans to intercept telephone calls.[10]

In 1997, four years after the FCC enacted congressionally mandated regulations banning the sale of scanning equipment capable of intercepting cellular signals,[11] a couple from Florida recorded a conference call between several senior Republican politicians, including then Speaker of the House Newt Gingrich, which they were able to intercept because one of the call's participants was using a cellular phone.[12] Although the couple did not intend to critique U.S. communications policy when they turned on their radio scanner, their act was high-profile proof that Congress' response to the analog interception threat was not successful.[13] What ultimately fixed the analog phone interception problem was not further congressional action but, rather, the wireless industry's migration away from easily intercepted analog

---

CELLULAR TELEPHONE CONVERSATIONS (1993) [hereinafter FCC REPORT AND ORDER], *available at* http://apps.fcc.gov/ecfs/document/view;jsessionid=CyspSn3R1KqpKlzyc9pwb5GyypnrQ4nnGMqFqtNpQyFYbhWZ2r1c!1357496456!-1864380355?id=1145780001 (made in response to Sec. 403 of the Telephone Disclosure and Dispute Resolution Act, Pub. L. 102-556 (1992)) (codified as amended at § 47 U.S.C. 302a(d) (requiring that within 180 days of enactment, the FCC shall prescribe and make effective regulations denying equipment authorization)). However, as the FCC made clear in its report, this prohibition does not apply to companies that "market[] [analog cellular interception technology] to law enforcement agencies . . . ." *Id*. at 7. Such a law enforcement exemption had been requested by the Harris Corporation, and supported by the cellular industry association. *See* CTIA REPLY COMMENTS, *supra* note 7, at 8 ("CTIA supports the Harris Corporation's request that the Commission modify its proposed rules to clarify that scanning receivers that receive cellular transmissions . . . may continue to be manufactured for sale to [law enforcement].").

10. *See* CTIA REPLY COMMENTS, *supra* note 7, at 3 (describing some commenters' concerns that "the Commission's proposed rules are flawed because they will not effectively safeguard the privacy of cellular calls" because "millions of scanning receivers capable of tuning cellular frequencies are already in use, and [] such receivers will remain available for sale for another year."); SUMMARY OF TESTIMONY OF THOMAS E. WHEELER, CELLULAR TELECOMM. INDUS. ASS'N: H. COMMERCE COMM., SUBCOMM. ON TELECOMMS., TRADE & CONSUMER PROT., 105th Cong. (1997) [hereinafter SUMMARY OF WHEELER TESTIMONY] (statement of Thomas E. Wheeler, Member, Cellular Telecomms. Indus. Ass'n) ("[T]rying to ban a specific type of eavesdropping gear after it has already become widely available is difficult.").

11. *See* FCC REPORT AND ORDER, *supra* note 9, at 1.

12. The participants of the call — who included Republican Majority Leader Dick Armey, Republican Whip Tom Delay, New York Congressman Bill Paxon, and Ohio Congressman John Boehner — were discussing an investigation of Gingrich by the Congressional Ethics Committee. The Florida couple gave the recording to the ranking Democratic member of the Ethics Committee (and thus the leader of the Gingrich investigation). *See The Gingrich Cellular Phone Call*, PBS NEWSHOUR (Jan. 14, 1997), http://www.pbs.org/newshour/bb/politics/jan-june97/cellular_01-14.html.

13. This was not the only opportunity in 1997 for Congress to observe that cellular communications were still not secure. *See* H.R. REP. NO. 105-425, at 5 (1998), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-105hrpt425/pdf/CRPT-105hrpt425.pdf ("The Subcommittee on Telecommunications, Trade, and Consumer Protection held a hearing on cellular privacy on February 5, 1997 . . . . Prior to the witnesses' testimony, a technological demonstration was conducted to highlight the ease with which scanning equipment can be 'readily altered' to intercept cellular communications.").

phone technology to digital cellular phones — a decision motivated in part by the increase in cellular phone cloning fraud.[14] Digital phone conversations were, at the time, far less likely to be intercepted because the necessary equipment was prohibitively expensive and thus available to fewer potential snoops.[15]

Governments with significant financial resources, however, have owned and used cellular phone surveillance equipment for quite some time.[16] Indeed, for nearly two decades, U.S. federal, state, and local law enforcement agencies have employed sophisticated cellular surveillance equipment that exploits vulnerabilities in cellular networks.[17] Once only accessible to a few global powers at six-figure prices, similar technology is now available to any government — including those with a history of spying in the United States — and to any other interested buyer from surveillance companies around the world, often for as little as a few thousand dollars per device.[18] Moreover, hobbyists can now build less advanced but functional interception equipment for as little as $100.[19] The normal course of economics and innovation has destroyed the monopoly a select group of global powers once enjoyed over digital cellular surveillance technology, rendering surreptitious access to cellular communications as universally available as it once was in the analog world. Surveillance has, once again, become democratized, this time with a much more expansive set of capabilities.

During congressional testimony in 1997, current FCC Chairman Tom Wheeler, then the president of the Cellular Telecommunications Industry Association ("CTIA"), warned the Committee of this outcome: "Unless Congress takes a forward-looking approach, history will likely repeat itself as digital scanners and decoders, though expensive now, drop in price in the future."[20] Mr. Wheeler's prescient warning has come true. Although the technology has changed, we are

---

14. Cell phone cloning is a process by which one phone's unique account number can be captured and programmed into another phone for purposes of billing one phone's calls to another phone. *See* Jeri Clausing, *Congress Moving Quickly To Try To Curb Cell Phone Abuses*, N.Y. TIMES (Mar. 2, 1998), http://www.nytimes.com/1998/03/02/business/congress-moving-quickly-to-try-to-curb-cell-phone-abuses.html.

15. *See* David Wagner et al., *Cryptanalysis of the Cellular Message Encryption Algorithm*, *in* ADVANCES IN CRYPTOLOGY — CRYPTO '97, at 526, 526 (1997), *available at* http://www.schneier.com/paper-cmea.pdf ("[T]he latest digital cellphones currently offer some weak protection against casual eavesdroppers because digital technology is so new that inexpensive digital scanners have not yet become widely available . . . ."); H.R. REP. NO. 105-425, *supra* note 13, at 3–4 ("While digital cellular and PCS are not immune from eavesdropping, they are currently more secure than analog cellular because the equipment for intercepting digital calls is vastly more expensive and complex than existing, off-the-shelf scanners that intercept analog communications (e.g., $200 vs. $10,000–$30,000).").

16. *See infra* Part V.A.

17. *See infra* Part III.

18. *See infra* Part V.

19. *Id*.

20. *See* SUMMARY OF WHEELER TESTIMONY, *supra* note 10.

rapidly approaching a future of widespread interception that feels like the past, but with a much larger range of public and private actors with more diverse motives for snooping. Whoever employs this technology can obtain direct, unmediated access to information about and from a cellular phone without any aid from a wireless provider.[21] In some cases, this technology can even intercept the contents of cellular phone calls, text messages, and other communications data transmitted to and from the phone.[22]

In this Article, we will argue that policymakers did not learn the right lesson from the analog cellular interception vulnerabilities of the 90s: That is, the communications of Americans will only be secured through the use of privacy-enhancing technologies like encryption, not with regulations prohibiting the use or sale of surveillance technology.

Nearly two decades after Congress passed legislation to protect analog phones from interception by radio scanners,[23] the American public is poised, quite unknowingly, at the threshold of a new era of communications interception that will be unprecedented in its pervasiveness and variety. Foreign governments, criminals, the tabloid press, and curious individuals with innumerable private motives can now leverage longstanding security vulnerabilities in our domestic cellular communications networks that were previously only exploitable by a few global powers.

In spite of the security threat posed by foreign government and criminal use of cellular surveillance technology, U.S. government agencies continue to treat practically everything about the technology as a closely guarded "source and method," shrouding the technical capabilities, limitations, and even the name of the equipment they use from public disclosure.[24] The source and method argument is invoked to protect law enforcement agencies' own use of cellular surveillance technology by preventing criminal suspects from learning how to evade monitoring and detection.[25] This secrecy is of questionable efficacy for that purpose, however, and it comes at a high collateral cost: For twenty years, the American public has been kept in the dark about

---

21. *See* John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 8, 2013), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/ ("The Sting[R]ay can grab some data from cellphones in real time and without going through the wireless service providers involved."); *Active GSM Interceptor: IBIS II — In-Between Interception System — 2nd Generation*, ABILITY COMPUTERS & SOFTWARE INDUS. LTD., http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html (last visited Dec. 18, 2014) [hereinafter *IBIS II*] ("The IBIS II is a stand-alone solution for off the air interrogation / interception / monitoring / deception of tactical GSM [(Global System for Mobile)] communication, in a seamless way, *without any cooperation with the network provider*.") (emphasis added).

22. *See infra* Part II.

23. *See* FCC REPORT AND ORDER, *supra* note 9.

24. *See infra* Part IV.

25. *See infra* Parts III.E, IV.

cellular network vulnerabilities and is thus generally unaware of the need to secure their private communications. Indeed, even though cybersecurity threats are a top congressional priority, it is only over the past year that a few policymakers have publicly acknowledged the exploitable vulnerabilities latent in our cellular networks, largely due to efforts by the press, privacy advocates, and researchers. Moreover, to date, there has been no corresponding serious policy debate about how to secure private communications from those threats.

If the United States and its close allies had a monopoly over this technology, the law enforcement community could credibly argue that certain national security interests furthered by the use of the technology — and thus the need to maintain the secrecy of all related information — trump the need to inform the American public about the vulnerability of cellular communications. This Article, however, dispels the myth that this technology is, in fact, secret at all. Indeed, it has been the subject of front page stories in leading newspapers,[26] has been featured in Hollywood movies[27] and television dramas,[28] and, more ominously, can be purchased over the Internet[29] from one of many non-U.S. based surveillance technology vendors or even built at home by hobbyists.[30] We therefore argue that the risks to the American public arising from the U.S. government's continued suppression of public discussion about vulnerabilities in our cellular communications networks that can be exploited to perform unmediated surveillance outweigh the now-illusory benefits of attempting to keep details of the technology secret. Congress should address these network vulnerabilities and the direct surveillance techniques they enable, as well as the necessity for responsive privacy-enhancing technologies like strong encryption,[31] as part of the larger cybersecurity debate, to

---

26. *See* Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, WASH. POST (Mar. 27, 2013), http://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html; Jennifer Valentino-DeVries, *"Stingray" Phone Tracker Fuels Constitutional Clash*, WALL ST. J. (Sept. 22, 2011), http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html.

27. *See* ZERO DARK THIRTY at 00:80:38 (Sony Pictures 2012).

28. *See The Wire: Middle Ground* at 00:12:57 (HBO television broadcast Dec. 12, 2004) (dialogue between two characters) ("Remember those analog units we used to use to pull cell numbers out of the air? . . . We used to have to follow the guy around, stay close while he used the phone." "New digitals . . . bing, we just pull the number right off the cell towers.").

29. *See* Letter from Rep. Alan M. Grayson to Tom Wheeler, Chairman, FCC (July 2, 2014), *available at* http://grayson.house.gov/images/pdf/rep_grayson_letter_to_federal_communications_commission_chairman.pdf (making reference to a Chinese online merchant and stating that "IMSI catchers can apparently 'be bought openly' from online retailers for as little as $1800").

30. *See infra* Part V.B.

31. *See* LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND

which they are all inextricably linked. To date, however, this policy debate is not occurring, which is not beneficial either to privacy or cellular network security.

Part II of this Article begins by naming this "secret" surveillance technology and describing its capabilities. Part III goes on to address the limited Department of Justice ("DOJ") guidance and case law pertaining to this technology. Part IV discusses what appears to be a concerted effort by the U.S. government to prevent the public disclosure of information about this technology. Part V reveals, however, that the existence of the technology is both publicly known and acknowledged by governments in other countries. Part VI describes how foreign governments and criminals can and do use cellular surveillance equipment to exploit the vulnerabilities in phone networks, putting the privacy and security of Americans' communications at risk. Part VII argues that the public is paying a high price for the U.S. government's perpetuation of a fictional secrecy surrounding cell phone surveillance technology. Specifically, such fictional claims of secrecy prevent policymakers from publicly addressing the threats to the security of cellular communications. Part VIII argues that cellular network vulnerabilities should be addressed publicly in the larger cybersecurity policy process Congress is currently undertaking. Finally, Part IX examines possible technical avenues through which solutions could come.

II. AN INTRODUCTION TO CELL PHONE SURVEILLANCE TECHNOLOGY

Because cellular telephones send signals through the air, cellular communications are inherently vulnerable to interception by many more parties than communications carried over a copper wire or fiber optic cable into a home or business.[32] This increased exposure to interception exists because anyone wishing to tap a traditional *wireline* telephone call must physically access the network infrastructure transporting that call — such as by attaching interception equipment to the telephone wires outside the home of the target or at the telephone company's central office.[33] In contrast, intercepting a cellular

---

COMMUNICATIONS TECHNOLOGIES 22 (2013), *available at* http://www.lawfareblog.com/wp-content/uploads/2013/12/Final-Report-RG.pdf (advising the U.S. government to "support[] efforts to encourage the greater use of encryption technology for data in transit, at rest, in the cloud, and in storage.").

32. *See* Timberg & Soltani, *supra* note 8 ("Cellphone conversations long have been much easier to intercept than ones conducted on traditional telephones because the signals are broadcast through the air, making for easy collection.").

33. *See id*. Carrier-assisted wiretaps once required that the interception take place near the target, such as at a call-switching center. Today, telephone carriers have modern interception equipment that permits intercepts to be remotely initiated and controlled by a single dedicated surveillance team within the companies. *See, e.g.*, UTIMACO, LAWFUL

telephone call only requires sufficient geographic proximity to the handset of one of the callers and the right kind of wireless interception equipment.

Cellular telephone calls can, of course, be intercepted by government agencies with the assistance of the wireless carriers via government-mandated interception capabilities these companies have built into their networks.[34] In fact, the vast majority of surveillance performed by law enforcement agencies in the United States is, almost certainly, carrier-assisted surveillance.[35] But cellular phone transmissions can also be captured without the assistance, or even the knowledge, of the carriers. The unmediated nature of this kind of interception, combined with the growing ease of access to cellular surveillance technology, makes the universe of private parties that can intercept a cellular call inestimably larger, and the range of their motives correspondingly broader, than the pool of potential law enforcement and national security actors who have both the legal capacity and technical capability to initiate a traditional wiretap of a wireline phone.

The technologies that enable the direct interception of cellular phone calls without the assistance of a wireless carrier generally fall into two categories: *passive* and *active*.[36] The former merely intercepts the signals sent between nearby phones and the wireless provider's network, while the latter transmits data to, and directly interacts with, the cellular phones under surveillance.

Passive interception technology functions in two stages. First, the signals exchanged between a cellular phone and the wireless carrier's network are intercepted as they are transmitted over the air. This pro-

---

INTERCEPTION OF TELECOMMUNICATION SERVICES, *available at* https://www.wikileaks.org/spyfiles/docs/UTIMACO-LIMSLawfInte-en.pdf (last visited Dec. 18, 2014) ("Utimaco's [Lawful Interception Management System] . . . automate[s] the administrative and operative tasks related to lawful interception. The system is based on a central management platform for the surveillance of communication services and implements electronic interfaces to various authorized law enforcement agencies and their monitoring centers."); ELAMAN, COMMUNICATIONS MONITORING SOLUTIONS, *available at* https://www.wikileaks.org/spyfiles/files/0/188_201106-ISS-ELAMAN3.pdf (last visited Dec. 18, 2014) ("Lawful Interception provides access to calls and call-related information (telephone numbers, date, time, etc.) within telecommunications networks, and delivers this data to a strategic Monitoring Center (MC) . . . . Such an MC gives access to an entire country's telecommunications network from one central place, but it needs the support of operators . . . .").

34. *See* The Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 (2012)) (requiring certain types of communications networks to contain built-in wiretapping capabilities).

35. *See* Eric Lichtblau, *Wireless Firms Are Flooded by Requests To Aid Surveillance*, N.Y. TIMES, July 9, 2012, at A1, *available at* http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html (describing the 1.3 million requests the wireless carriers received in 2011 from law enforcement agencies).

36. *See* Karsten Nohl & Chris Paget, *GSM — SRSLY?*, 26TH CHAOS COMM. CONG. (26C3) (Dec. 27, 2009), http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf.

cess does not disrupt the signals in transit. Second, once intercepted, if the communications are encrypted, they must be decrypted for analysis.[37] Not all communications are encrypted in transmission but, if they are, the ease of decryption varies based on the strength of the encryption algorithm chosen by the wireless carrier.[38] As described in greater detail in Part V of this Article, the major Global System for Mobile communications ("GSM") network operators in the U.S., such as AT&T and T-Mobile, still use extremely weak encryption algorithms for their older, second generation ("2G") networks which can be easily deciphered with widely available software or purpose-built hardware.[39] Moreover, although the competing code division multiple access ("CDMA") cellular networks (operated by Verizon and Sprint) use different, incompatible cellular technology and encryption algorithms, surveillance companies offer products capable of intercepting and tracking CDMA phones too.[40]

---

37. Encrypted cellular communications must be decrypted before they can be listened to. In some countries, like India, encryption between phones and the network base stations is disabled. In India, this is a result of legislation prohibiting the use of encryption, likely intended to make interception by the government easier. *See* Nehaluddin Ahmad, *Restrictions on Cryptography in India — A Case Study of Encryption and Privacy*, 25 COMPUTER L. & SEC. REV. 173, 175 (2009); Pranesh Prakash, *How Surveillance Works in India*, N.Y. TIMES (July 10, 2013), http://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india/ ("[P]roviders in India have been known [to] use A5/0, that is, no encryption . . . ."). In the United States, there is no law requiring wireless carriers to use encryption to protect calls. The choice is left entirely up to the carriers, which do use encryption in some cases, but not always. *See infra* Part V.B.3.

38. A number of encryption algorithms are supported by modern cellular telephone systems, but the specific algorithm used to encrypt communications between a telephone and the carriers' network is chosen by the wireless carrier. In the United States, the A5/1 algorithm and A5/0 (the "NULL" encryption option) are still used by major GSM carriers, such as AT&T and T-Mobile, for their 2G networks. *See infra* Part V. The major CDMA carriers, Sprint and Verizon, use different encryption algorithms for their 2G and 3G networks. The Long Term Evolution ("LTE") 4G cellular standard, which is the next generation technology adopted by all U.S. carriers, includes support for encryption algorithms that are much stronger. However, as with prior generations of cellular technology, wireless carriers can still choose to not use any encryption (the NULL option) with LTE. *See* VERIZON, THE VERIZON WIRELESS 4G LTE NETWORK: TRANSFORMING BUSINESS WITH NEXT-GENERATION TECHNOLOGY 16 (2012), *available at* http://business.verizonwireless.com/content/dam/b2b/resources/LTE_FutureMobileTech_WP.pdf ("The 128-bit AES algorithm is the preferred option in the Verizon Wireless 4G LTE network . . . . AES is preferred because it has undergone more public scrutiny than other encryption options.").

39. See *infra* Part V for a discussion of the software tools and commercial products now available to crack cellular encryption algorithms.

40. These include the Harris Corporation and Elaman. *See* Letter from Lin Vinson, Major Account Manager of Wireless Prods. Grp., Harris Corp., to Raul Perez, City of Miami Police Dep't (Aug. 25, 2008), *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/48003.pdf ("The Harris StingRay and KingFish systems are compatible with the CDMA standard . . . ."); HARRIS CORPORATION, STINGRAY PRODUCT DESCRIPTION, *available at* http://files.cloudprivacy.net/Harris_Stingray_product_sheet.pdf (last visited Oct. 24, 2014) (describing one version of the Harris StingRay as a "Transportable CDMA Interrogation, Tracking and Location, and Signal Information Collection System"); ELAMAN, *supra* note 33, at 14 ("For operational field usage, off-air GSM monitoring systems are very powerful and essential . . . . Systems for . . . CDMA are [also] available.");

Active surveillance, performed with a device known as an *International Mobile Subscriber Identity* ("*IMSI") catcher* or *cell site simulator*, works by impersonating a wireless base transceiver station ("BTS") — the carrier-owned equipment installed at a cell tower to which cellular phones connect — and tricking the target's phone into connecting to it.[41] For some surveillance capabilities, such as intercepting communications content, the IMSI catcher can also impersonate the carrier's network infrastructure, such that calls and text messages are transmitted through the IMSI catcher, once again without disrupting the communication and thus remaining imperceptible to the target.[42] Depending on the particular features of the surveillance device and how they are configured by the operator, IMSI catchers can be used to identify[43] nearby phones, locate them with extraordinary precision,[44] intercept outgoing calls and text messages,[45] as well

Advanced CDMA Interception System, INTERCEPT MONITORING SYS., http://en.intercept.ws/catalog/2197.html (last visited Dec. 18, 2014).

41. *See* Daehyun Strobel, IMSI Catcher 13 (July 13, 2007) (unpublished seminar paper, Ruhr-Universitat Bochum), *available at* http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf ("An IMSI Catcher exploits [GSM's lack of authentication] and masquerades to a Mobile [Phone] as a Base Station.").

42. *See, e.g.*, ABILITY COMPUTERS & SOFTWARE INDUS. LTD., IBIS (IN-BETWEEN INTERCEPTION SYSTEM) PRODUCT DESCRIPTION 4, *available at* http://www.toplinkpac.com/pdf/IBIS_Brochure.pdf (last visited Oct. 24, 2014) ("IBIS can fully imitate target's phone and talks with GSM network on its behalf . . . . Such a scheme makes *possible interception of incoming and outgoing calls* . . . .") (emphasis added).

43. *See, e.g.*, CELLXION LTD., UGX SERIES 330: TRANSPORTABLE DUAL GSM / TRIPLE UMTS FIREWALL AND ANALYSIS TOOL, *available at* http://s3.documentcloud.org/documents/810703/202-cellxion-product-list-ugx-optima-platform.pdf (last visited Oct. 24, 2014) (including as features, "[c]omprehensive identification of IMSI, IMEI and TMSI information" and "[s]imultaneous high speed acquisition of handsets (up to 1500 per minute), across up to five networks"); *Septier IMSI Catcher*, SEPTIER COMMC'N LTD., http://www.septier.com/146.html (last visited Dec. 18, 2014) ("Septier IMSI Catcher allows its user to extract the IMSI and IMEI of GSM MS operating in its coverage area . . . .").

44. *See, e.g.*, Memorandum from Stephen W. Miko, Resource Manager, Anchorage Police Dep't, to Bart Mauldin, Purchasing Officer, Anchorage Police Dep't (June 24, 2009) [hereinafter Miko Memorandum], *available at* http://files.cloudprivacy.net/anchorage-pd-harris-memo.pdf ("[The] system allows law enforcement agencies . . . the ability to . . . [i]dentify location of an active cellular device to within 25 feet of actual location anywhere in the United States."); HARRIS CORPORATION, AMBERJACK PRODUCT DESCRIPTION, *available at* http://egov.ci.miami.fl.us/Legistarweb/Attachments/34769.pdf (last visited Dec. 18, 2014) ("AmberJack is a phased array direction finding (DF) antenna system capable of tracking and locating mobile phone users. The DF antenna array is designed to operate with Harris' Loggerhead and StingRay products . . . ."); PKI ELECTRONIC INTELLIGENCE GMBH GERMANY, GSM CELLULAR MONITORING SYSTEMS 12, http://www.pki-electronic.com/2012/wp-content/uploads/2012/08/PKI_Cellular_Monitoring_2010.pdf (last visited Dec. 18, 2014) (describing device's ability to locate "a target mobile phone with an accuracy of 2 m[eters].").

45. *See, e.g.*, *IBIS II*, *supra* note 21 (noting the ability to intercept "incoming and outgoing [calls]"); VERINT, TACTICAL OFF-AIR INTELLIGENCE SOLUTIONS 15 (2013), *available at* http://s3.documentcloud.org/documents/885760/1278-verint-product-list-engage-gi2-engage-pi2.pdf (describing device's ability to "[l]isten to, read, edit, and reroute incoming and outgoing calls and text messages").

as block service, either to all devices in the area or to particular devices.[46]

Cellular surveillance technology, by its very nature, tends to be invasive and over-broad in its collection of data.[47] Active surveillance devices send signals, often indiscriminately, through the walls of homes,[48] vehicles, purses, and pockets in order to probe and identify the phones located inside.[49] Both active and passive devices also pick up the signals of other phones used by innocent third parties, particularly when government agencies using them do not know the exact location of their target and thus must drive through cities and neighborhoods while deploying cellular surveillance equipment in order to locate her.[50]

Both passive and active telephone surveillance technologies exploit security flaws in cellular telephones. Passive devices exploit the weak or, in some cases, lack of any encryption used to protect calls, text messages, and data transmitted between phones and the wireless carriers' base stations. Active surveillance devices, on the other hand, exploit the lack of authentication of the base station by cellular phones.[51] As a result, phones have no way to differentiate between a legitimate base station owned or operated by the target's wireless carrier and a rogue device impersonating a carrier's base station.[52]

---

46. *See* CELLXION LTD., *supra* note 43 (describing device's ability to "[d]isable all handsets except operationally friendly"); Miko Memorandum, *supra* note 44 ("[The] system allows law enforcement agencies . . . the ability to . . . [i]nterrupt service to active cellular connection [and] [p]revent connection to identified cellular device.").

47. In some cases, this may be a selling point. *See* VERINT, *supra* note 45, at 7 (describing product's ability to "collect mass GSM traffic over a wide area").

48. The devices send signals like those emitted by a carrier's own base stations. Those signals, of course, must "penetrate walls" to provide connectivity indoors. *What You Need to Know About Your Network*, AT&T, http://www.att.com/gen/press-room?pid=14003 (last visited Dec. 18, 2014); E.H. Walker, *Penetration of Radio Signals into Buildings in the Cellular Radio Environment*, 62 BELL SYS. TECHNICAL J. 2719 (1983).

49. *See* Kelly, *supra* note 21 ("Typically used to hunt a single phone's location, the system intercepts data from all phones within a mile, or farther, depending on terrain and antennas.").

50. *See* Affidavit of Supervisory Special Agent Bradley S. Morrison at 5, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC) [hereinafter Morrison Affidavit 2012], *available at* http://www.documentcloud.org/documents/1282619-11-10-17-2011-u-s-v-rigmaiden-cr08-814-phx-dgc.html ("During a location operation, the electronic serial numbers (ESNs) (or their equivalent) from all wireless devices in the immediate area of the FBI device that subscribe to a particular provider may be incidentally recorded, including those of innocent, non-target devices.").

51. *See* Strobel, *supra* note 41, at 13.

52. More recent cellular phone systems, including so-called 3G and 4G networks, now include the capability for phones to authenticate the network base stations. *See generally* Muxiang Zhang & Yuguang Fang, *Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol*, 4 IEEE TRANSACTIONS ON WIRELESS COMMC'NS 734, 734 (2005), *available at* http://www.fang.ece.ufl.edu/mypaper/tw05zhang.pdf. However, even the latest smartphones are backward compatible with older, vulnerable phone network technologies, which allows the phone to function if it is taken to a rural location or foreign country where the only service offered is 2G. As a result, modern phones remain vulnerable to active surveillance via a *protocol rollback attack* in which the nearby 3G and 4G network

Passive wireless surveillance devices do not transmit any signals.[53] These devices are thus far more covert in operation — indeed effectively invisible[54] — but they can only detect signals of nearby phones when those phones are actually transmitting data.[55] Active surveillance devices have the disadvantage of being relatively less covert because they produce telltale signals that are detectable using sophisticated, counter-surveillance equipment,[56] but their corresponding advantage is that they can rapidly identify and locate all nearby phones that are turned on, even if they are not transmitting any data.[57]

A. An Approximate History of Cellular Phone Surveillance Technology[58]

Rohde & Schwarz, a German manufacturer of radio equipment, is generally believed to have created the first purpose-built active device capable of performing surveillance on cellular telephones.[59] Their first model, introduced in 1996, identified nearby wireless telephones by

---

signals are first jammed. *See* Matthew Green, *On Cellular Encryption*, A FEW THOUGHTS ON CRYPTOGRAPHIC ENGINEERING (May 14, 2013), http://blog.cryptographyengineering.com/2013/05/a-few-thoughts-on-cellular-encryption.html ("The biggest . . . concern for 3G/LTE is that you may not be using it. Most phones are programmed to gracefully '*fail over*' to GSM when a 3G/4G connection seems unavailable. Active attackers exploit this feature to implement a *rollback attack* — jamming 3G/4G connections, and thus reactivating all of the GSM attacks . . . .").

53. *See GTReS — GSM Traffic Recording System*, ABILITY COMPUTERS & SOFTWARE INDUS. LTD., http://www.interceptors.com/intercept-solutions/Passive-GSM-Interceptor.html (last visited Dec. 18, 2014) (describing product as "a multi-band fully passive GSM interception system" which "is completely undetectable").

54. *See* VERINT, *supra* note 45, at 7 (describing product's ability to "[o]perate undetected leaving no electromagnetic signature").

55. Any phone that is connected to a cellular network will regularly transmit data to nearby base stations, even if it is not making calls, sending text messages, or using the Internet. Locating a phone that is not currently transmitting data with a passive interception device may, however, require waiting some time until the device "checks in" with the cellular network or otherwise communicates with a nearby base station.

56. *See infra* Part IV.C.

57. *See* CELLXION LTD., *supra* note 43.

58. As telephone interception technology is also used by intelligence agencies and the military, it is impossible to tell a totally accurate history of the development of wireless telephone interception technology. As with many surveillance technologies, the military and intelligence community are the first to use them, and, after time, they trickle down to law enforcement. Neither the manufacturers of this equipment nor their many intelligence and military clients advertise their use. This portion of our Article is an attempt to paint an approximate picture, but it is likely that there are many aspects to this story that are missing, due to the fact that they remain classified.

59. The earliest public document describing IMSI catchers and the Rohde & Schwarz products is an article in 1997 by Dirk Fox, a German security consultant. *See* Dirk Fox, *IMSI-Catcher*, 21 DATENSCHUTZ UND DATENSICHERHEIT 539, 539 (1997), *available at* http://www.secorvo.de/publikationen/imsi-catcher-fox-1997.pdf. Five years later, Fox published an updated, more in-depth article about the same technology. *See* Dirk Fox, *Der IMSI-Catcher*, 26 DATENSCHUTZ UND DATENSICHERHEIT 212, 212 (2002), *available at* http://www.secorvo.de/publikationen/imsicatcher-fox-2002.pdf.

forcing them to transmit their serial number, or IMSI.[60] Within a year, the company had introduced a more sophisticated product that could also intercept outgoing phone calls.[61]

U.S. government agencies have used both active and passive forms of cellular telephone surveillance technology since at least the early 1990s, if not earlier.[62] Military and intelligence agencies were early adopters of this technology, with law enforcement agencies quickly following their lead.[63] Passive devices, often referred to as *digital analyzers*, were used by law enforcement agencies as early as 1991.[64] Active surveillance devices were also used by federal law enforcement agencies as early as 1995.[65] Initially, U.S. agencies used devices that were "general use" cell site simulators, which wireless carrier technicians operated to test cellular phones.[66] Later, cellular equipment manufacturers created and sold cell site simulators specifically designed for government surveillance.

Infamous computer hacker Kevin Mitnick was located in 1995 by FBI agents using a combination of an active cell site simulator and a passive *TriggerFish*, a digital analyzer manufactured by the Harris Corporation.[67] The active cell site simulator was able to page Mitnick's phone without causing an audible ring,[68] after which the passive TriggerFish was used to locate the phone.[69]

By 2003, Harris had introduced its more sophisticated StingRay product,[70] which performed active surveillance of digital cellular

---

60. *See* Strobel, *supra* note 41, at 13; MMI Research Ltd v. Cellxion Ltd & Ors, [2009] EWHC (Pat) 418, [130] (Eng.), *available at* http://www.bailii.org/ew/cases/EWHC/Patents/2009/418.html (describing a presentation of the Rohde & Schwarz GA-090 IMSI Catcher device to three German wireless carriers in December 1996).

61. *See* Strobel, *supra* note 41, at 13.

62. As U.S. law enforcement and intelligence agencies do not advertise their intelligence gathering sources and methods, there is no way to accurately determine when U.S. government agencies first started to use active or passive wireless phone surveillance technology.

63. *See* Kelly, *supra* note 21 ("Initially developed for military and spy agencies, the Sting[R]ays remain a guarded secret by law enforcement and the manufacturer, Harris Corp. of Melbourne, Fla.").

64. *See* Glen L. Roberts, *Who's on the Line? Cellular Phone Interception at Its Best*, FULL DISCLOSURE (1991), *available at* http://blockyourid.com/~gbpprorg/2600/harris.txt (describing the marketing by the Harris Corporation of TriggerFish passive surveillance devices to law enforcement agencies at the National Technical Investigators Association conference in 1991).

65. *See* Tsutomu Shimomura, *Catching Kevin*, WIRED, Feb. 1996, at 124, *available at* http://www.wired.com/wired/archive/4.02/catching_pr.html.

66. *Id*.

67. *Id*.

68. This capability is commonly referred to as a "silent SMS." *See generally* Fabien Soyez, *Getting the Message? Police Track Phones with Silent SMS*, OWNI.EU (Jan. 27, 2012), http://owni.eu/2012/01/27/silent-sms-germany-france-surveillance-deveryware.

69. Shimomura, *supra* note 65.

70. The U.S. Trademark office registration of StingRay, registered in 2003, described the device as a "multi-channel, software-defined, two-way electronic surveillance radio[] for authorized law enforcement and government agencies for interrogating, locating, tracking

telephones.[71] The company now manufactures an extensive range of cellular telephone surveillance products,[72] which can be mounted in vehicles, on airplanes and drones, or carried by a person.[73] Harris sells its products to local, state, and federal law enforcement agencies,[74] intelligence agencies, and the military.[75] The company dominates the U.S. law enforcement market, although several other companies also sell similar technology to U.S. military and intelligence agencies.[76]

---

and gathering information from cellular telephones . . . ." STINGRAY, Registration No. 2,762,468.

71. *See* HARRIS CORPORATION, *supra* note 40 ("StingRay is Harris' latest offering in a long line of advanced wireless surveillance products. StingRay is a multichannel software defined radio that performs network base station surveys, Dialed Number and registration collection, mobile interrogation, and target tracking and location with Harris' AmberJackTM Direction-Finding Antenna.").

72. *See* Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

73. *See* Jennifer Valentino-DeVries, *Judge Questions Tools that Grab Cellphone Data on Innocent People*, WALL ST. J. (Oct. 22, 2012), http://blogs.wsj.com/digits/2012/10/22/judge-questions-tools-that-grab-cellphone-data-on-innocent-people/; Freedom of Information Act Response from U.S. Immigration and Customs Enforcement to author (Sept. 19, 2012) [hereinafter Freedom of Information Act Response], *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/479397/stingrayfoia.pdf (describing the purchase of a "StingRay II Airborne Training" session and an "Airborne Flight Kit").

74. *See* Kelly, *supra* note 21 ("At least 25 police departments own a Sting[R]ay, a suitcase-size device that costs as much as $400,000 and acts as a fake cell tower . . . . In some states, the devices are available to any local police department via state surveillance units.").

75. *See, e.g.*, Space and Naval Warfare Systems Command, *Harris Corp Blackfin Equipment*, FEDBIZOPPS.GOV (May 24, 2010), https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=f34fc14f76e8744bfe75d41e6d0242db; U.S. Army Intelligence and Security Command, *Notice of Intent To Award a Sole Source Contract-Harris: KingFish Dual Mode System*, FEDBIZOPPS.GOV (Jan. 12, 2009), https://www.fbo.gov/index?s=opportunity&mode=form&id=fd03ebae781f3a3fdb7633699bc1e351&tab=core&_cview=1; *Customized Equipment Training (SET017)*, MARINE CORPS INTELLIGENCE SCHOOLS, https://www.mcis.usmc.mil/ITEP/Lists/ITEP%20Course%20Catalogue/DispForm.aspx?ID=31 (last visited Dec. 18, 2014) (including "Harris Corporation: Gossamer, LongShip, BlackFin, BlackFin II, HawksBill, SpurDog, FishFinder, KingFish, StingRay, StingRay II, GSM Interrogator, CDMA Interrogator, iDEN Interrogator, UMTS Interrogator, FishHawk, Porpoise, FireFish, Tarpon, AmberJack, Harpoon, Moray, LanternEye, RayFish, StoneCrab"); U.S. Marine Corps, *Interrogation, Tracking, Location and Signal Information Collection System Devices with Software and Training*, FEDBIZOPPS.GOV (Sept. 12, 2006), https://www.fbo.gov/index?s=opportunity&mode=form&id=6a5efbcce2b7bdf2f37448ad68d48e7e&tab=core&_cview=0; U.S. Special Operations Command, *FishHawk Software*, FEDBIZOPPS.GOV (Sept. 22, 2011), https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=3176fb4a66f92793ac34e7670205e2c5 ("StingRay II — Special Equipment — Over-The-Air special signal software that is compatible with the Harris StingRay II System.").

76. Other manufacturers of cellular surveillance technology used by the U.S. military and intelligence agencies include Boeing, CellXion, and Martone Radio Technology. Comments of the Boeing Company, to the Nat'l Telecomm. & Info. Admin., U.S. Dep't of Commerce, Preventing Contraband Cell Phone Use in Prisons, 75 Fed. Reg. 26733 (May 12, 2010), *available at* http://www.ntia.doc.gov/files/ntia/comments/100504212-0212-01/attachments/Boeing%20and%20DRT%20Comments%20on%20NTIA%20Contraband%20Cell%20Phone%20NOI%206%2011%2010.pdf ("DRT [(a wholly owned subsidiary of Boeing)] manufactures a line of wireless location and management technologies that emulate a base

B. Uses of Direct Surveillance Technology

Law enforcement agencies perform most cellular surveillance with the assistance of telecommunications and Internet companies. This method of surveillance uses carrier-owned equipment or technology that enables surveillance — typically with the aid of dedicated electronic surveillance and compliance teams employed by these companies.[77] For more than one hundred years, the telephone companies have provided such assistance.[78] While carrier-performed or enabled surveillance is generally the easiest, most efficient, and most covert way to intercept communications, it is not the only way.[79]

In spite of the user-friendly, often inexpensive surveillance capabilities provided to the government by wireless carriers,[80] there are certain situations where governments may need or prefer to engage in

---

station to detect and locate wireless handsets of interest in a limited geographic area."); FCC Application for New or Modified Radio Station by Phoenix Global Support (Mar. 21, 2011), *available at* https://apps.fcc.gov/oetcf/els/reports/442_Print.cfm?mode=current&application_seq=47486&license_seq=48001 (requesting a license to use transmitting devices made by Martone Radio Technology, Harris, and CellXion). Phoenix Global Support, the company that requested the license, is located less than fifteen miles from Fort Bragg, in Fayetteville, NC, the headquarters of the Joint Special Operations Command ("JSOC"). The company's website states that it "offers complete classes and curriculum for Signals Intelligence (SIGINT) and Electronic Warfare (E/W) spanning the spectrum of wireless communications." PHOENIX GLOBAL SUPPORT, www.pgsup.com (last visited Dec. 18, 2014).

77. *See* Letter from William B. Petersen, Gen. Counsel, Verizon Wireless, to Rep. Edward J. Markey (May 22, 2012), *available at* http://web.archive.org/web/20121217111531/http://markey.house.gov/sites/markey.house.gov/files/documents/Verizon%20Wireless%20Response%20to%20Rep.%20Markey.pdf ("Verizon Wireless has a dedicated team of approximately seventy that works . . . to respond to lawful demands for customer information . . . ."); Letter from Timothy P. McKone, Exec. Vice President, Fed. Relations, AT&T, to Rep. Edward J. Markey (May 29, 2012), *available at* http://web.archive.org/web/20121228183409/http://markey.house.gov/sites/markey.house.gov/files/documents/AT%26T%20Response%20to%20Rep.%20Markey.pdf ("AT&T employs more than 100 full time workers . . . for the purpose of meeting law enforcement demands.").

78. By 1895, the New York Police Department had the ability to wiretap any telephone in the city. Wes Oliver, Wiretapping and the Apex of Police Discretion (Apr. 22, 2010) (Widener Law School Legal Studies Research Series, Paper No. 10-14), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1594282 (describing "the early years of police wiretapping," where "a police officer would simply go to the telephone company and request that the phone company assist them with a wiretap," which allowed the wiretap squad to "listen-in on any telephone call in the City of New York.").

79. In fact, since the earliest days of the telephone, the police have also directly performed wiretaps. *See* Meyer Berger, *Tapping the Wires*, THE NEW YORKER, June 18, 1938, at 41, *available at* http://www.spybusters.com/History_1938_Tapping_Wires.html ("In those days police wire-tappers just walked into the Telephone Company's offices, asked for the location of the wires they were interested in, and got the information without fuss. Lines were usually tapped right in the cellar of the house or at an outside wall box.").

80. *See* Christopher Soghoian, *ACLU Docs Reveal Real-Time Cell Phone Location Spying Is Easy and Cheap*, SLIGHT PARANOIA (Apr. 3, 2012), http://paranoia.dubfire.net/2012/04/aclu-docs-reveal-real-time-cell-phone.html (quoting Paul Taylor, Electronic Surveillance Manager, Sprint Nextel, as stating that Sprint's web-based GPS tracking tool is extremely popular with law enforcement, who "love that it is extremely inexpensive to operate and easy").

direct, unmediated surveillance of telephones themselves using an active or passive device. These situations include:

(1) Identifying unknown phones currently used by a known target. In situations where a surveillance target is believed to frequently switch phones (for example, by using so-called "burner" disposable phones[81]), investigators may wish to learn the serial number of the phone currently in use, which is necessary in order to initiate a carrier-assisted wiretap[82] or Pen Register/Trap and Trace device (hereinafter Pen/Trap).[83] Law enforcement can determine the specific phone used by a particular surveillance target by deploying an IMSI catcher to collect data about nearby phones at multiple locations, such as the target's home and place of business. This method ultimately narrows the search to only those phones that were present in all of the monitored locations.[84]

(2) Locating devices that cannot be found by the wireless carriers. Federal E-911 regulations require that carriers be able accurately to determine the location of cellular phones.[85] As this technical obligation was mandated in the context of E-911,[86] it only applies to

---

81. *See The Wire: Hamsterdam* at 00:42:23 (HBO television broadcast Oct. 10, 2004) (dialogue between two characters) ("They make a few calls with a burner, throw it away. Go on to the next phone, do the same. There's more of those things laying around the streets of West Baltimore than empty vials." "Well, how the fuck you supposed to get a wire up on that?").

82. *See* 18 U.S.C. §§ 2511–2520 (2012) (authorizing the interception of wire, oral, or electronic communications — including communications content — by law enforcement to investigate crimes enumerated in the statute upon satisfying various elements set out in the statute).

83. *See* 18 U.S.C. §§ 3121–3127 (2012) (authorizing law enforcement to install and use a pen register device to "record[] or decode[] [non-content] dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted" and to install and use a trap and trace device to "capture[] the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication . . . .").

84. *See* Complaint at 8 n.1, United States v. Chaparro, No. 12 CR 969, 2014 BL 216188 (N.D. Ill. Aug. 5, 2014), *available at* http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf ("[L]aw enforcement officers . . . used a digital analyzer device on three occasions in three different locations where Chaparro was observed to determine the IMSI associated with any cellular telephone being carried by Chaparro."); *The Wire: Middle Ground* at 00:18:20 (dialogue between two characters) ("[I]f we know the approximate time of [the target's] call we can start just by pulling calls off that tower, at that time." "That could be thousands." "Yeah, but that's the baseline, but we get a second hit . . . and that list comes down to dozens. And after a third or fourth . . . then we've got his number.").

85. *See* 47 C.F.R. § 20.18(h) (2014).

86. *Id*. Similarly, although CALEA only required the wireless carriers to turn over information about the cell sites used at the beginning and end of a call, *supra* note 34, federal law enforcement agencies subsequently asked the FCC to issue regulations requiring the carriers to be able to turn over higher-accuracy location E-911 location information at any time, without the knowledge of the subscriber. *See* FED. COMMC'NS COMM'N, PETITION FOR EXPEDITED RULEMAKING, IN THE MATTER OF PETITION FOR EXPEDITED RULEMAKING TO ESTABLISH TECHNICAL REQUIREMENTS AND STANDARDS PURSUANT TO SECTION 107(B) OF

devices capable of making a telephone call to 911. As such, there is no affirmative obligation that wireless carriers be able to accurately locate data-only devices, such as tablet computers and mobile data-cards. When the government wishes to locate data-only devices that cannot be precisely located by the wireless carrier,[87] it is likely to turn to active cellular surveillance.

(3) Selectively blocking devices or dialed numbers. There are situations and environments where public safety officials may use a cell site simulator to selectively block the use of particular phones.[88] Some prisons, for example, have installed devices that permit access to registered phones, such as those used by guards and other staff, while blocking all unregistered phones, such as those smuggled into the facility, from making or receiving calls.[89] Law enforcement agencies may also, during high-security events like a hostage situation or a bomb threat, seek to redirect outgoing numbers dialed by particular phones or block incoming calls to all nearby phones.

(4) Foreign intelligence and military operations. Although U.S. government agencies can compel surveillance assistance from U.S. wireless carriers, this power does not extend to telephone companies in foreign countries. Moreover, even if some level of assistance is available from foreign governments, U.S. agencies may wish to keep their foreign surveillance activities covert, such as when the surveil-

---

THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT 27, 32, 37 (2007), *available at* http://askcalea.fbi.gov/lef/docs/20070823_JSTD025-BDeficiencyPetition Wappendices.pdf (stating that since the carriers now have E-911 mandated high-quality location data, they should be required to deliver it to law enforcement). The FCC never acted on this petition, but, perhaps under pressure from law enforcement, many major wireless carriers now provide law enforcement real-time E-911 GPS level accuracy location data. *See* Soghoian, *supra* note 80 (describing the real-time GPS tracking surveillance tools offered by several wireless carriers).

87. The FCC gave wireless carriers the choice of using *handset-based* or *network-based* technology to comply with the E-911 mandate. *See* FED. COMMC'NS COMM'N, THIRD REPORT AND ORDER, NO. 99-245, IN THE MATTER OF REVISION OF THE COMMISSION'S RULES TO ENSURE COMPATIBILITY WITH ENHANCED 911 EMERGENCY CALLING SYSTEMS (1999), *available at* http://transition.fcc.gov/Bureaus/Wireless/Orders/1999/fcc99245.pdf. The handset-based solution involves the installation in telephone handsets of GPS chips that can be remotely queried. In contrast, the network-based solution requires the installation of specialized technology at the carriers' base stations, which can then locate any device connected to the carrier's network, including data-cards and tablet computers. As such, carriers such as AT&T and T-Mobile, which have deployed network-based E-911 technology, are able to locate data-devices, while Verizon and Sprint, which deployed handset-based E-911 technology, cannot. *See id*.

88. *See* Miko Memorandum, *supra* note 44 ("The KingFish Dual-Mode System . . . is a . . . cellular phone surveillance and tracking system . . . . This system allows law enforcement agencies . . . to . . . [i]nterrupt service to active cellular connection [and] [p]revent connection to identified cellular device ('No Service').").

89. *See* NAT'L TELECOMM. AND INFO. ADMIN., U.S. DEP'T OF COMMERCE, REP. ON CONTRABAND CELL PHONES IN PRISONS, POSSIBLE WIRELESS TECHNOLOGY SOLUTIONS 19–25 (2010), *available at* http://www.ntia.doc.gov/files/ntia/publications/contrabandcellphonereport_december2010.pdf (describing "managed access" methods of preventing contraband cell phones from being used in prisons).

lance is aimed at a particular foreign government and its political leaders.[90] As a result, when conducting surveillance abroad — and in some cases, even domestically[91] — direct surveillance technology may be the most effective surveillance (or even the only) tool available to U.S. intelligence agencies and military units for intercepting certain communications or tracking particular phones.[92] The same logic, of course, applies to foreign governments conducting espionage in the United States.[93]

III. "KNOWN KNOWNS": CASE LAW AND DOJ GUIDANCE

U.S. law enforcement agencies have used cellular surveillance technology for more than two decades[94] and spent tens of millions of dollars acquiring these devices at federal, state, and local levels.[95]

---

90. *See* Duncan Campbell et al., *Revealed: Britain's "Secret Listening Post in the Heart of Berlin,"* INDEPENDENT (Nov. 5, 2013), http://www.independent.co.uk/news/uk/home-news/revealed-britains-secret-listening-post-in-the-heart-of-berlin-8921548.html; *How NSA Spied on Merkel Cell Phone from Berlin Embassy*, DER SPIEGEL (Oct. 27, 2013), http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html ("From the roof of the embassy, a special unit of the CIA and NSA can apparently monitor a large part of cellphone communication in the government quarter. And there is evidence that agents based at Pariser Platz recently targeted the cellphone that [German Chancellor Angela] Merkel uses the most.").

91. When performing surveillance on sophisticated targets with counter-intelligence expertise, such as foreign embassies and foreign intelligence services operating from foreign embassies in the U.S., intelligence agents are likely to use passive cellular interception technology because it is far more difficult to detect. *See* Matthew M. Aid, *Spy Copters, Lasers, and Break-In Teams*, FOREIGN POLICY (Nov. 19, 2013), http://www.foreignpolicy.com/articles/2013/11/19/spy_copters_lasers_and_break_in_teams_fbi_spies_on_diplomats (describing FBI "vans, aircraft, and helicopters" that are "*equipped with equipment capable of intercepting cell-phone calls and other electronic forms of communication*" for the purpose of "intercept[ing] the communications of all diplomatic missions and international organizations located on American soil" (emphasis added)).

92. *See* Jeremy Scahill & Glenn Greenwald, *The NSA's Secret Role in the U.S. Assassination Program*, INTERCEPT (Feb. 10, 2014), https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/ (describing NSA drones equipped with "'virtual base-tower transceivers' . . . that can force a targeted person's device to lock onto the NSA's receiver" and allow "the military to track the cell phone to within 30 feet of its actual location, feeding the real-time data to teams of drone operators who conduct missile strikes or facilitate night raids.").

93. *See infra* Part VI.

94. *See supra* Part II.A (discussing the fact that law enforcement has used passive devices since at least 1991 and active devices since at least 1995).

95. *See* Freedom of Information Act Response, *supra* note 73 ("ICE has invested $5,000,000.00 towards the investment of equipment and training in Harris Corporation services."); Kelly, *supra* note 21 ("The federal government funds most of the [StingRay] purchases, via anti-terror grants."); Marisa Kendall & John Kelly, *Cell Tower Dumps Not Used Locally*, NEWS-PRESS, Dec. 8, 2013, at A, *available at* https://www.aclu.org/sites/default/files/assets/news-press_article_131208.pdf ("[The Florida Department of Law Enforcement] has spent more than $3 million buying a fleet of Sting[R]ays, records show."); Carl Prine, *FBI Closely Guards Details of Spy Gear Technology*, PITT. TRIB.-REV. (Feb. 16, 2014), http://triblive.com/news/allegheny/5548583-74/fbi-technology-projects (stating that public records revealed that Harris "secured 68 FBI contracts worth at least $23.7 million.

Notwithstanding this history, there is scant case law addressing its use in investigations. Indeed, when compared with traditional, carrier-assisted cellular phone tracking,[96] there is limited case law and publicly available internal agency guidance describing: (1) statutory authorities that may permit or preclude law enforcement use and how the DOJ interprets such authorities to permit or limit law enforcement use (to include any Fourth Amendment constraints); (2) the frequency or regularity with which such technology is used by federal, state, and local law enforcement; (3) the types of investigations or actual factual scenarios where law enforcement agencies have used the technology; and (4) any related prosecution-based and policy-driven considerations for the retention of data collected by an IMSI catcher. This Part will present and analyze the limited publicly available case law and DOJ guidance in an attempt to describe the policies and rules governing federal law enforcement agencies' use of this technology.

A. The 1995 Digital Analyzer Magistrate Opinion[97]

Despite their use since at least 1991,[98] it was not until 1995 that a federal magistrate judge in California published the first decision analyzing a government application to use a digital analyzer.[99] In this matter, the government wanted court authorization to use a passive surveillance device to "analyze signals emitting from any cellular phone used by any one of five named subjects of a criminal investigation."[100] The agents likely needed to use this technology because they did not know the particular phone numbers that the targets were using, and thus could not seek surveillance assistance from the targets' wire-

---

Purchases included Harris devices such as the StingRay, Amberjack, Kingfish and Gossamer trackers, plus spare parts and classroom instruction.").

96. For a discussion of the statutory authorities used by law enforcement to acquire cellular phone location data and an analysis of multiple court opinions addressing law enforcement access to location data, see generally Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117 (2012). For information about the frequency or regularity with which federal, state, and local law enforcement agencies make requests for location data from carriers, see generally the collection of documents posted at http://www.markey.senate.gov/documents/2013-10-03_ATT_re_Carrier.pdf and http://www.markey.senate.gov/documents/2013-12-09_VZ_CarrierResponse.pdf (describing carrier disclosure of real-time and historical location data to law enforcement agencies).

97. Our analysis of this magistrate opinion draws from our previous article, Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH 134, 157–60 (2013).

98. *See* Roberts, *supra* note 64.

99. In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197 (1995). The government submitted an *ex parte* application for an order permitting agents of the Orange County Regional Narcotics Suppression Program ("RNSP") to use a digital analyzer. *Id*. at 198–99.

100. *Id*. at 199.

less carriers.[101] It also appears that the agents wanted to determine with whom the targets were communicating, information they could obtain in real time by intercepting signals as calls took place.[102]

Following what was likely DOJ policy at the time,[103] the government sought a pen register order authorizing the surveillance. Magistrate Judge Edwards denied the government's application without prejudice, explaining that a Pen/Trap court order was not required because the Pen/Trap statute limits its application "to a device 'which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line *to which such device is attached*.'"[104] Judge Edwards noted that, because the digital analyzer was not intended to be — and could not be — physically attached to the cellular phone, the Pen/Trap statute was not applicable to its use.[105]

---

101. The opinion notes that agents could not identify the particular cellular telephones they wished to analyze. *Id*.

102. *Id*. Information about whom targets are communicating with is often relevant to identifying the scope of the alleged criminal activity to discover the identities of additional criminal targets that may not be known to law enforcement. It would not, however, be necessary for the agents to continue to use a digital analyzer to determine the phone numbers the target phone was calling and was called by once the target phone was identified through its unique identifying number. Rather, agents could subpoena historical telephone toll records from the relevant cell phone provider(s) or obtain a Pen/Trap order to collect real-time records from the provider(s) reflecting this information. Indeed, once target phones are appropriately identified through their unique numbers, more traditional forms of carrier-assisted surveillance can proceed.

103. *See* discussion *infra* Part III.B.

104. *See* In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. at 200.

105. *Id*. The court further explained its reasoning:

> The statutory definition of a "trap and trace device" does not include the limitation in the definition of a pen register described above, limiting the devices to those that are attached to a telephone line. *See* 18 U.S.C. § 3127(4). Nonetheless, it appears from the construction of related sections of the statutes governing trap and trace devices that they include only devices that are attached to a telephone line. Specifically, 18 U.S.C. § 3123(b) requires that an order for use of both pen registers and trap and trace devices include "the number and, if known, physical location *of the telephone line to which the pen register or trap and trace device is to be attached* . . . ."
>
> This limitation on the proscription against pen registers and trap and trace devices to prohibit only devices that are "attached" to a telephone line cannot be assumed to be inadvertent. In other statutes relating to interceptions of telephone communications, Congress encompassed, generally, any types of interceptions of wire, oral, or electronic communications — regardless of whether the intercepting device was "attached" to a telephone line. *See, e.g*., 18 U.S.C. § 2511. That Congress did not impose equally comprehensive restrictions on lesser interceptions that do not raise 4th Amendment issues, such as those made with pen registers and trap and trace devices, is neither surprising nor inconsistent.
>
> In any event, it must be remembered that the prohibition against the use of pen registers and trap and trace devices without court order is found in a criminal statute. *See* 18 U.S.C. § 3121(d).

Judge Edwards also found, pursuant to the third party doctrine as articulated in *Smith v. Maryland*,[106] that the government's use of a digital analyzer raised no Fourth Amendment concerns.[107] The court noted that "[n]umbers dialed by a telephone are not the subject of a reasonable expectation of privacy" and "[n]o logical distinction is seen between telephone numbers called and a party's own telephone number (or [device serial] number), all of which are regularly voluntarily exposed and known to others."[108]

Although Judge Edwards ruled that the Pen/Trap statute did not regulate the passive surveillance technology the government sought to use — that is, it neither authorized nor prohibited its use — he expressed serious reservations about its use by law enforcement.[109] Specifically, he expressed concern about both the privacy of innocent third parties in range of the device and a lack of adequate congressional oversight.[110] If the court were to authorize the government's use of a digital analyzer to identify the particular phones used by known targets, Judge Edwards acknowledged that such an order would essentially permit agents to intercept signals emitted from *all* phones in the target's area.[111] Thus, in addition to the unique serial numbers identifying the targets' phones, the digital analyzer would also identify the serial numbers of phones used by innocent third parties.[112] Judge Edwards recognized that "depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted."[113]

> Under well-settled principles, the statute should be strictly construed, and any ambiguity in its scope must be construed narrowly.

Id.

106. 442 U.S. 735 (1979).

107. In the Matter of the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. at 199.

108. *Id*.

109. *Id*. at 201–02.

110. *Id*.

111. *Id*.

112. *Id*.

113. *Id*. at 201. The court also noted that, although the agents were not seeking to intercept communications content, the digital analyzer they used could be programmed for that purpose. *Id*. at 199; *see also* STAFF OF THE ELEC. SURVEILLANCE UNIT, OFFICE OF ENFORCEMENT OPERATIONS — ITS ROLE IN THE AREA OF ELECTRONIC SURVEILLANCE 14 (1997) [hereinafter 1997 DOJ GUIDANCE] (published in the U.S. Attorneys' Bulletin), *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf (describing a digital analyzer as being "programmed so it will not intercept cellular conversations or dialed numbers when it is used for the limited purpose of seizing ESNs and/or the cellular telephone's number," although the analyzer is capable of such interceptions); ELEC. SURVEILLANCE UNIT, U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 41 (2005) [hereinafter 2005 ELECTRONIC SURVEILLANCE MANUAL], *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf ("Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be

The court also expressed concern that an order, if granted, would permit the government to collect data about large numbers of phones without any record-keeping or reporting requirements, thus preventing effective congressional oversight of the surveillance tool. Specifically, the court contrasted the "lack of record production" with the statutory reporting requirements in the Pen/Trap statute, such as "the use of court orders that identified particular telephones and the investigative agency" and "periodic reports to Congress stating the numbers of such orders."[114] Noting these differences and others,[115] the court found that the government's application "would not insure sufficient accountability."[116]

Although clearly troubled by the surveillance capabilities of this technology, the court could not restrain its use by law enforcement.[117] Moreover, the court's determination that neither the Fourth Amendment nor the Pen/Trap statute authorized, restricted, or otherwise regulated law enforcement use of the technology likely reinforced the DOJ's view that it did not *need* court authorization for use of a digital analyzer, even if it advised prosecutors to seek court authorization out of an abundance of caution or as a matter of policy.[118] The DOJ later articulated this position in a 1997 internal document.

B. The 1997 DOJ Guidance

A document published by the DOJ in 1997, initially distributed nationally to prosecutors[119] and later published on the DOJ's website, is the earliest publicly available DOJ document that describes the capabilities of passive and active wireless phone surveillance technology.[120] The document also discusses, again for the first time, the legal

---

configured to disable the interception function, unless interceptions have been authorized by a Title III order.").

114. *See* In re the Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. at 201–02.

115. *Id*. (citing 18 U.S.C. §§ 3123(b), 3126).

116. *Id*. at 201.

117. The court denied the government's application because it found that the Pen/Trap statute was not applicable to a digital analyzer. *Id*. at 200. The court noted that the government was seeking the application only "'out of an abundance of caution.'" *Id*.

118. The court's reasoning appears to illustrate its concern that, if it granted such an order — even "'out of an abundance of caution'" — pursuant to a statute whose definitional elements did not conform to the surveillance technique at issue, the court risked giving: (1) a potentially incorrect interpretation of a statute, or worse (2) judicial approval of a surveillance technique that Congress appeared neither explicitly to authorize nor prohibit.

119. *See* 1997 DOJ GUIDANCE, *supra* note 113. USA Bulletins are published by the Executive Office of United States Attorneys ("EOUSA") and distributed to United States Attorneys' Offices across the country. They cover a range of topics and issues of interest to federal prosecutors (such as law enforcement surveillance methods), including new case law, law enforcement tools and practices, statutory authorities, and internal DOJ guidance.

120. *Id*. at 13–14 (describing the types of information that digital analyzers and cell site simulators acquire).

policies governing the technology's use by federal law enforcement agents.[121]

In this document, the DOJ took the position that, as long as (1) law enforcement agents were not intercepting communications content and (2) the acquisition of the non-content data did not involve the assistance of carriers, "it does not appear that there are constitutional or statutory constraints on the warrantless use of [an active or passive surveillance] device . . . ."[122] In other words, the DOJ appears to have recognized no need for a warrant or other judicial process for

---

121. *Id*. at 13–15.

122. *Id*. at 14. Specifically, the DOJ reasoned that

> Title III's provisions (18 U.S.C. §§ 2510-2522) would not apply to the use of a digital analyzer or a CSS when they are used to capture call processing information (MIN, ESN, cell site location, status of call, etc.) because they do not intercept the contents of any wire, oral, or electronic communication as the term "contents" is defined by Title III. Currently, Section 2510(8) states, "'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that information." ESNs/MINs and other automatic call processing information that are technologically necessary for the service provider to process cellular calls are not the types of transmissions Congress included within Section 2510(8)'s definition of "contents" when it was amended in 1986. [See S. Rep. No. 541 at 13 (1986)].

Id. (bracketed citation in original). Moreover, the DOJ asserts:

> [T]here is no "electronic communication" [as defined by 18 U.S.C. § 2510(12)] unless the MIN or ESN is "transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce." A transmission normally contemplates a sender and a receiver. The ECPA legislative history regarding the definition of wire communication warns against an improper mechanical reading of the phrase "in whole or in part . . . by the aid of wire . . ." and states that the phrase "is intended to refer to wire that carries the communication to a significant extent from the point of origin to the point of reception, even in the same building. It does not refer to wire that is found inside the terminal equipment at either end of the communication." [S. Rep. No. 99-541, 12.] Thus, it does not appear that MINs and ESNs "forced" from the cellular telephone by the CSS or obtained by a digital analyzer are "electronic communications" within the contemplation of 18 U.S.C. § 2510(12).

Id. (bracketed citations in original). The DOJ further excludes collection of cell site information from a digital analyzer or cell site simulator from Stored Communications Act ("SCA") statutory requirements:

> If cell site information is treated as a subscriber record or other information rather than a contemporaneous electronic communication covered by Title III, then 18 U.S.C. § 2703 (regarding stored electronic communications) might apply. It should be noted, however, that Section 2703 controls disclosures by service providers to Government entities and does not prohibit the Government from obtaining such information on its own without involving the service provider. Additionally, because CSSs and digital analyzers do not access communications in electronic storage in a facility with electronic communication service, Section 2703 does not apply.

Id. at 14–15.

law enforcement's use of digital analyzers and cell cite simulators when they are only employed to intercept non-content data (including location data and real-time numbers sent and received) without the assistance of carriers, whether in relation to specific targets or innocent third parties.

Although concluding that law enforcement use of these direct, unmediated surveillance devices did not *require* any legal process, the 1997 DOJ Guidance, as a matter of *policy*, advises that "to the extent [cell site simulators] and digital analyzers are used as pen registers or trap and trace devices, they should only be used pursuant to a court order issued pursuant to these statutes."[123] When law enforcement wants to determine in real time the calls made and received by a particular phone, the government can obtain a court order compelling a service provider to install a pen register or trap and trace device.[124] This disclosure of information involving carrier assistance is regulated by statute, whereas the digital analyzer and cell site simulator technology enables government agents to obtain the same information directly from cell phones *without* any statutory process requirement. Perhaps in an effort to reconcile this disparity in regulation, arguably as early as 1995[125] but certainly by 1997, the DOJ advised prosecutors and agents to seek Pen/Trap court process when using a digital analyzer/cell cite simulator as a Pen/Trap device.[126]

The 1997 DOJ Guidance also recognized that digital analyzers and similar technologies could capture cell site location data (to include cell cite data for target phones as well as innocent third-party phones).[127] While the capability to acquire location data directly may not have raised significant constitutional or policy-related "red flags" to the DOJ in 1994[128] or 1997, determining and fixing the proper legal

123. *Id*. at 14 (noting that the guidance to seek a Pen/Trap order is "[d]epartment[] policy").

124. *See* 18 U.S.C. §§ 3121–3127 (2012).

125. The DOJ sought a Pen/Trap order from Judge Edwards "out of an abundance of caution." *See supra* note 117.

126. 1997 DOJ GUIDANCE, *supra* note 113, does not, however, give any similar guidance with respect to direct (non-carrier assisted) collection of cell phone location data. In other words, it does not advise agents and prosecutors to obtain the same legal process used to compel location data from carriers.

127. *Id*. at 14. Digital analyzers and cell site simulators "can capture the cell site codes identifying the cell location and geographical sub-sector from which the cellular telephone is transmitting; the call's incoming or outgoing status; the telephone numbers dialed (pen register order required); and the date, time, and duration of the call." *Id*.

128. In 1994, the Office of Enforcement Operations ("OEO") opined that "investigators did not need to obtain any legal process in order to use cell phone tracking devices so long as they did not capture the numbers dialed or other information 'traditionally' collected using a pen/trap device." 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 45. Back in 1994, the OEO concluded that the "'signaling information' automatically transmitted between a cell phone and the provider's tower does not implicate either the Fourth Amendment or the wiretap statute because it does not constitute the 'contents' of a communication." *Id*. Moreover, the 1994 analysis reasoned that "the pen/trap statute did not

standard(s) for authorizing law enforcement access to location data has become the subject of considerable debate for both the courts and Congress.[129]

C. The 2001 USA PATRIOT Act Amendments to Pen/Trap Statute and Guidance in the 2005 Electronic Surveillance Manual

While the PATRIOT Act is generally not thought of as privacy-enhancing legislation, it did bring law enforcement use of passive and active cellular surveillance technology under some limited degree of judicial supervision and congressional oversight through specific definitional changes to the Pen/Trap statute.

Whereas the pre-2001 pen register definition only applied to "numbers dialed or otherwise transmitted," the PATRIOT Act added the term "signaling information."[130] The 2005 edition of the DOJ's Electronic Surveillance Manual explains that "'[s]ignaling information' is a broader term that encompasses other kinds of non-content information used by a communication system to process communications."[131] Indeed, the DOJ instructed prosecutors that the new pen register definition "appears to encompass *all* of the non-content between a cell phone and a provider's tower."[132]

---

apply to the collection of such information because of the narrow definitions of 'pen register' and 'trap and trace device.'" *Id*. Therefore, "since neither the [C]onstitution nor any statute regulated their use, such devices did not require any legal authorization to operate." *Id*.

129. *See generally* Pell & Soghoian, *supra* note 96 (describing the current congressional debates over proper legal standard(s) and analyzing various magistrate opinions requiring different legal standards for law enforcement access to location data).

130. *See* 18 U.S.C. § 3127(3) (2012) (defining pen register as "a device or process which records or decodes dialing, routing, addressing, and signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted").

131. 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 45

132. *Id*. (emphasis added). Similarly, the definition of "trap and trace" device, which originally included only "the originating number of an instrument or device" expanded to include "the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication . . . ." 18 U.S.C. § 3127(4). Like the expanded definition of pen register, the DOJ instructs that the new trap and trace definition now "appears to include such information as the transmission of a MIN [or other type of unique identifying number], which identifies the source of a communication." 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 46. The DOJ's conclusion that Pen/Trap now encompasses all non-content data between a cell phone and a cell tower was based, in part, on its analysis of the relevant but "scant" legislative history which suggested that the new definitions were intended to "apply to all communications media, instead of focusing solely on traditional telephone calls." *Id*. Examining, for example, House language referencing "a packet requesting a telnet session — a piece of information passing between machines in order to establish a communication session for the human user," the DOJ suggests that the term "provides a close analogy to the information passing between a cell phone and a tower in the initial stages of a cell phone call." *Id*. at 47. Moreover, in contrast to earlier Pen/Trap definitions that referenced the attachment of a Pen/Trap device to a phone line, the House Report recognized that Pen/Trap devices "could . . . collect information remotely." *Id*.

These expanded Pen/Trap definitions had implications for law enforcement's direct collection of mobile device serial numbers, real-time monitoring of numbers called and received, and acquisition of location information. Specifically, post-PATRIOT Act, the DOJ took the position that *all* forms of non-content data collected directly required prosecutors to obtain a Pen/Trap court order.[133]

D. 2012 Cell Site Simulator ("StingRay") Magistrate Opinion[134]

With the passage of the PATRIOT Act in 2001, the DOJ took the position that a Pen/Trap order was necessary to authorize law enforcement use of direct surveillance technology, like a StingRay, to intercept non-content data. It would take more than a decade, however, for a federal magistrate judge to publish an opinion evaluating an

---

It should be noted, however, that the DOJ drew a distinction between standards authorizing "off air" collection of cell phone location data via digital analyzers and IMSI catchers and the collection of these data through *compelled disclosures* from carriers. Indeed, in 1994, the CALEA instructed that "any information that may disclose the physical location of [a telephone service] subscriber" may *not* be acquired "solely pursuant to the authority for pen registers and trap and trace devices . . . ." 47 U.S.C. § 1002(a)(2) (2012). The DOJ opined that, "[b]y its very terms, this prohibition applies only to information collected by a provider and not to information collected directly by law enforcement authorities. Thus, CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate targeted cell phones." 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 46–47.

As applied to compelled disclosures of prospective location information from carriers, the CALEA dictate meant that the DOJ had to find another authority to pair with or replace Pen/Trap authority. Since at least 2005, the DOJ has been advising prosecutors to obtain both a Pen/Trap order and an 18 U.S.C. § 2703(d) order ("D Order"). *See* Pell & Soghoian, *supra* note 96, at 135–37. Moreover, some magistrate judges have required "probable cause" search warrants before issuing orders authorizing law enforcement to compel a provider to track a cell phone in real time. *Id*. at 137–39. As referenced earlier, the appropriate standard(s) for law enforcement-compelled disclosures of historical and prospective location data remains an unresolved issue for the courts and Congress. *See supra* note 96. For purposes of this discussion, however, it is sufficient to note that both a D Order and a "probable cause" warrant standard are more stringent than Pen/Trap. To obtain a Pen/Trap order, the government need merely certify that the information sought "is relevant to an ongoing criminal investigation . . . ." 18 U.S.C. § 3122(b)(2) (2012). Such "certification" does not require any fact finding by a magistrate judge. *See* Pell & Soghoian, *supra* note 97, at 155–56. In contrast, to obtain a D Order, the government must assert and a judge must find "specific and articulable facts" that the location information sought is "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The requirement for a search warrant is even more stringent, as the government must show, and a magistrate must find, that there is probable cause to believe that the location information would be "evidence of a crime." *See* FED. R. CRIM. P. 41(c)(1). Notwithstanding that compelling location data from a carrier would require a more stringent standard than that found in the Pen/Trap statute, the DOJ's 2005 Guidance took both the legal and policy position that a Pen/Trap order was sufficient for direct collection of cell phone location data by law enforcement. 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 47 ("CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate targeted cell phones.").

133. *Id*. at 45–48.

134. Our analysis of this magistrate opinion draws from our previous article. Pell & Soghoian, *supra* note 97.

application for law enforcement use of a direct, active surveillance device.[135]

In 2012, a federal magistrate judge from Texas issued an order denying an application submitted by agents from the Drug Enforcement Agency for the use of a StingRay.[136] The government sought a Pen/Trap order "to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones . . . ."[137] The agents submitted their application pursuant to 18 U.S.C. §§ 3122(a)(1), 3127(5) (the Pen/Trap statute) and 2703(c)(1) (a provision of the Stored Communications Act).[138] The government informed Magistrate Judge Owsley that the application was "based on a standard application model and proposed order approved by the [DOJ]."[139]

Since the subject was known to law enforcement (whereas the subject's phone was unknown), the agents planned to identify the phone by capturing device identification data "at various locations in which the [subject's] [t]elephone [was] reasonably believed to be operating . . . ."[140] After reviewing the application, Judge Owsley conducted an *ex parte* hearing and ultimately denied the government's application.[141] Judge Owsley expressed concern that the application did not explain adequately either the technology itself, "how many distinct surveillance sites [the agents] intend[ed] to use, or how long

---

135. One likely reason for this time gap is the default sealing of all pen register applications and orders with no corresponding requirement that they be unsealed outside of the prosecution's discovery obligations to indicted criminal defendants as part of the criminal discovery process. *See generally* Stephen Wm. Smith, *Gagged, Sealed and Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 314 (2012) ("Through a potent mix of indefinite sealing, nondisclosure (i.e., gagging), and delayed-notice provisions, ECPA [Electronic Communications Privacy Act] surveillance orders all but vanish into a legal void."). The Pen/Tap statute is Title III of ECPA. *See* Pub. L. No. 99-508, tit. III, 100 Stat. 1848, 1868–73 (codified as amended at 18 U.S.C. §§ 3121–3127 (2012)).

136. In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012). A target had switched from using a phone known to agents to an unknown phone. *Id*. The agent leading the investigation indicated that the "equipment designed to capture [the] cell phone numbers was known as a '[S]ting[R]ay.'" *Id*.

137. *Id*.

138. It is not clear from the 2012 magistrate opinion what purpose this citation to ECPA's Stored Communications Act served in terms of providing additional authority of unmediated, direct collection of non-content data in this investigation. The 2005 Guidance indicated that only a Pen/Trap order was required for use of devices to collect non-content data directly. 2005 ELECTRONIC SURVEILLANCE MANUAL, *supra* note 113, at 47–48. The DOJ, however, might have provided updated guidance reflecting a different or more nuanced legal position. As of the writing of this Article, this new guidance, if it exists, is not publically available.

139. In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d at 749.

140. *Id*. at 748.

141. *Id*. at 748, 752.

they intend[ed] to operate the [S]ting[R]ay equipment to gather all telephone numbers in the immediate area."[142] Moreover, the court noted that no explanation was given, either in writing or verbally, as to what would be done with the innocent information collected from the phones of uninvolved individuals who just happened to be in the area under surveillance.[143] Finally, the court expressed concern that neither the prosecutor nor the Drug Enforcement Administration agent appeared to understand the technology at issue and "seemed to have some discomfort in trying to explain it."[144]

Notwithstanding these concerns, the court's decision to deny the application appears to stem from a definitional problem the court identified in the Pen/Trap statute that the government did not adequately address during the application or *ex parte* hearing process. While recognizing that the PATRIOT Act broadened the Pen/Trap definitions, "amplif[ying] the various types of information that are available such as routing and signaling information,"[145] Judge Owsley interpreted § 3123(b)(1) of the pen register statute as "straightforward in that a telephone number or similar identifier is *necessary* for a pen register."[146] Accordingly, the judge found that the language in the statute "mandates that this Court have a telephone number or some similar identifier before issuing an order authorizing a pen register."[147] Because the government did not provide any support to the contrary in case law or any other authority suggesting that the statute authorized collection of non-content data from *unidentified* devices, the judge denied the application without prejudice.[148]

E. The Rigmaiden Federal Prosecution

In 2011, a decade after the Harris Corporation introduced the StingRay,[149] the FBI's use of the device finally surfaced during the pre-trial stages of a criminal case.[150] The government prosecuted Daniel David Rigmaiden ("Rigmaiden") for his role in a scheme through which he obtained fraudulent tax refunds for hundreds of deceased

142. *Id*. at 749.
143. *Id*.
144. *Id*.
145. *Id*. at 751.
146. *Id*. (emphasis added).
147. *Id*.
148. *Id*. at 751–52.
149. *See* discussion *supra* Part II.
150. United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012); *see also* Valentino-DeVries, *supra* note 26 ("A [S]ting[R]ay's role in nabbing the alleged 'Hacker' — Daniel David Rigmaiden —is shaping up as a possible test of the legal standards for using these devices in investigations.").

persons and other third parties.[151] After a lengthy investigation, federal agents located Rigmaiden, in part by tracking the location of "[a wireless data-card] connected to a laptop computer" in his apartment.[152] The government did not know Rigmaiden's actual identity until agents arrested him.[153] Indeed, the government's only solid lead was an IP address associated with the prepaid Verizon data-card that Rigmaiden used to transmit fraudulent tax returns to the IRS.[154] To narrow down the location of the data-card, the government obtained historical cell-site records from Verizon. Those records determined that the data card's location was within an approximately one-quarter square-mile area. As Verizon did not have the technical capability to provide higher-accuracy location information,[155] the government used a StingRay to locate the data-card, leading the agents to Rigmaiden's apartment.[156]

Prior to locating the data-card, the government obtained a search warrant pursuant to Fed. R. Crim. P. 41(b) authorizing the use of a cell site simulator.[157] After his arrest, Rigmaiden filed a motion to suppress, arguing that the government had repeatedly violated the Fourth Amendment in its efforts to locate him.[158] Ultimately, the gov-

---

151. The government indicted Rigmaiden in a superseding indictment on seventy-four counts of wire fraud, aggravated identify theft, mail fraud, and conspiracy to commit these offenses. United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *1 (D. Ariz. May 8, 2013). In April 2014, Rigmaiden pleaded guilty to four felony counts of mail fraud, wire fraud, and conspiracy to commit these offenses. *See* Dennis Wagner, *Tax Scammer Rigmaiden Pleads Guilty, Gets Time Served*, AZCENTRAL (Apr. 8, 2014), http://www.azcentral.com/story/news/politics/2014/04/07/rigmaiden-tax-scammer-pleads-guilty/7448151. He was sentenced to time served, which amounted to the sixty-eight months he spent awaiting trial. *Id*.

152. United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *1 (D. Ariz. May 8, 2013).

153. *Id*. at 1–6.

154. *Id*. at 1–4.

155. *See supra* Part II.B.2 and note 86 (explaining how E-911 regulations do not require carriers to be able to locate data-only devices in real-time).

156. Investigative Details Report at 7, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC), *available at* https://ia600707.us.archive.org/33/items/gov.uscourts.azd.396130/gov.uscourts.azd.396130.484.6.pdf (U.S. Postal Inspection Services Inspector James L. Wilson states in the report that "[o]n 7/16/08, we were informed that they were able to track a signal and were using a 'Sting[R]ay' to pinpoint the location of the aircard.").

157. United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013) (noting that Judge Seeborg found that the warrant application "established 'probable cause to believe that the use and monitoring of a mobile tracking device' would 'lead to evidence of' several specific crimes, including conspiracy to defraud the government, fraud relating to identity information, aggravated identity theft, and wire fraud," and the identification of those who committed the offenses).

158. Rigmaiden's motion to suppress divides the government's investigative actions into twenty-one different searches. *Id*. at 6. In its Order addressing Rigmaiden's Motion to Suppress, the District Court grouped the alleged searches, the defendant's challenges, and the government's responses into the following categories:

> whether Defendant had a legitimate expectation of privacy in the location of the aircard; the government's collection of historical cell-

ernment conceded *arguendo* that its efforts to locate Rigmaiden's data-card constituted a Fourth Amendment search and seizure.[159]

A key question to consider is why the government chose to make this concession when the DOJ's 2005 Guidance did not advise that digital analyzers and cell site simulators raised any Fourth Amendment issues that would necessitate securing a warrant. Is there a more nuanced DOJ position directing or advising prosecutors to obtain a warrant when the use of a cell site simulator may reveal the location of a device to be inside a home or other protected space?[160]

> site information, destination IP addresses, and data from the Domicilio apartment's alarm company; the search for the aircard using the mobile tracking device; the searches of Defendant's apartment and computer; and whether the Fourth Amendment's good faith exception applies.

Id. at 6–7.

159. *Id*.; Government's Memorandum Re Motion for Discovery at 1, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC); s*ee also* United States v. Rigmaiden, 844 F. Supp. 2d 982, 996–97 (D. Ariz. 2012). In an order addressing the defendant's motion to suppress, the District Court isolated certain facts related to the use of the cell site simulator, some of which were stipulated to by the government, including: (1) signals sent by the mobile tracking device to the aircard are signals that would not have been sent to the aircard in the normal course of Verizon's operation of its cell towers, (2) the tracking operation was a Fourth Amendment search and seizure, and (3) the mobile tracking device located the aircard precisely within Defendant's apartment. *Id*. at 14.

160. *See* Reporter's Transcript of Proceedings: Motion Hearing at 61, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC). During questioning by the judge, prosecutors explained:

> We generally recommend [the] use [of] a search warrant at a point where we think that we're going to reasonably be interrogating a device within an area where there's a reasonable expectation of privacy, because we're — in going into that area where there's a reasonable expectation of privacy, we want to ensure a neutral and detached magistrate has made a finding of probable cause at that point.
>
> However, it's the same type of data that we're getting in both missions, because based upon the transmissions back and forth to the cell tower is what we would use to direction-find the cellular device.
>
> With a pen register order, we — because the pen register order doesn't include a finding of probable cause by a magistrate, we will generally restrict our use there to where we're not knowingly going into an area where there's a reasonable expectation of privacy . . . .
>
> . . . .
>
> . . . . It's not the nature of the data; it's the nature of the interest. And the — the nature of the — the legal interests, the Fourth Amendment — you know, where you have an expectation of privacy is where we would recommend using the search warrant as opposed to just a pen register order.

Id. (statement by Mr. Mazel). Indeed, the prosecutors recognized that Kyllo v. United States, 533 U.S. 27, 40 (2001), where the Supreme Court held that "[g]overnment use[] [of] a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion . . . is a 'search' and is presumptively unreasonable without a warrant," would likely apply to the government's use of a StingRay to send a signal though walls of an apartment complex to locate Rigmaiden's data-card. *See*

If the DOJ anticipated *actual* Fourth Amendment issues with its use of a cell site simulator to locate Rigmaiden, obtaining a warrant was a reasonable, prudent precaution. The government's *arguendo* concession, however, is limited to the defendant's motion to suppress in the instant case. In other words, the DOJ did not take the position, *arguendo* or otherwise, that law enforcement use of a StingRay in any other criminal investigation would constitute a Fourth Amendment search. Moreover, the government seems to shift positions on whether it believes the Fourth Amendment was implicated during some part of the tracking operation to locate Rigmaiden: At first, it suggested that (notwithstanding the *arguendo* concession) the tracking operation, "as a factual matter . . . did not involve a search or seizure under the Fourth Amendment."[161] Later during direct questioning from the court, however, the government explained that it seeks a warrant when a cell site simulator would locate an individual in a protected space.[162] Ultimately, the 2011 Rigmaiden prosecution provides no clarity about the government's view on when or if the use of a Sting-Ray requires an agent to obtain a warrant.

Indeed, in late 2014, the Wall Street Journal revealed that the U.S. Marshals Service has equipped airplanes with IMSI catchers, which, since 2007, the agency has flown over cities to locate targets.[163] The IMSI catchers used in these tracking operations interact with and collect data from a vast number of innocent people's phones.[164] Moreover, such surveillance necessarily involves sending signals through the walls of homes and apartment buildings or penetrating briefcases, purses, and pockets in order to identify the phones contained within. While the Rigmaiden case presented a situation where law enforcement agents canvassed a neighborhood (and thus penetrated with electronic signals many of the homes within that neighborhood),[165] the U.S. Marshals' airplane-assisted surveillance operations involve surveillance on a much larger scale. Indeed, they send signals into huge numbers of Fourth Amendment protected spaces — potentially into every home, purse, and pocket in a city. Such dragnet surveillance operations therefore raise serious legal questions, even if authorized by a court.[166]

Reporter's Transcript of Proceedings: Motion Hearing at 63, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

161. Government's Memorandum Re Motion for Discovery at 1 n.1, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

162. *See* Reporter's Transcript of Proceedings: Motion Hearing, *supra* note 160.

163. Devlin Barrett, *Americans' Cell Phones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014), http://online.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

164. *Id*.

165. *See supra* note 156 and accompanying discussion in main text.

166. *See, e.g.*, [Proposed] Brief Amici Curiae in Support of Daniel Rigmaiden's Motion to Suppress at 17, United States v. Rigmaiden, 844 F. Supp. 2d 982, 989 (D. Ariz. 2012)

While it is impossible to discern all elements behind the DOJ's concession in Rigmaiden's case, one aspect of the rationale emerges in the discovery, pre-trial motion practice, and related hearings: The government considers cell site simulator technology to be a sensitive source and method that it believes will be rendered less effective if its capabilities were revealed publicly, as future targets of surveillance would learn how to thwart the surveillance method. Accordingly, prosecutors appear to have made strategic choices to limit the StingRay's exposure in the case, including an effort to protect the device's name.[167] In response to certain Rigmaiden discovery requests, for example, the government argued that the technology used to locate the Defendant's data-card and the manner in which the technology was employed was "sensitive law enforcement information"[168] subject to the qualified privilege recognized in *Roviaro* and *Van Horn*.[169] These cases essentially hold that the government can shield information about sensitive investigative techniques when a court determines that such disclosure would not be relevant or helpful to the defense or otherwise "essential to a fair determination of a cause . . . ."[170]

Hence, while Rigmaiden filed discovery motions to compel the government to disclose more information about the cell site simulator,[171] the government's concession that the tracking operation was a Fourth Amendment search presumably foreclosed the relevance of at least some details about the StingRay and its use by law enforcement (thereby preventing their public disclosure).[172] That the government

(No. 2:08-CR-008814-DGC) ECF No. 904-3, *available at* https://www.aclu.org/files/assets/rigmaiden_amicus.pdf ("That [S]ting[R]ays obtain information about third parties 'creates a serious risk that every warrant for [a StingRay] will become, in effect, a general warrant,' to search persons as to whom there is no probable cause.").

167. *See* Morrison Affidavit 2012, *supra* note 50, at 1 ("The actual make and model of the equipment used in any particular operation by the FBI is law enforcement sensitive, and pursuant to FBI policy, cannot be released to the general public.").

168. United States v. Rigmaiden, 844 F. Supp. 2d 982, 989 (D. Ariz. 2012).

169. *Id*. at 2 (citing Roviaro v. United States, 353 U.S. 53 (1957) and United States v. Van Horn, 789 F.2d 1492 (11th Cir. 1986)).

170. *Roviaro*, 353 U.S. at 60–61. With respect to government surveillance equipment, the defendant-target of electronic surveillance is not entitled to learn the location and type of equipment used by the government unless he can show sufficient need for such information. *Van Horn*, 789 F.2d 1492.

171. *See* Motion for Additional Discovery Due to Government Ignoring Defendant's Recent Discovery Requests, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

172. *See* Government's Memorandum Re Motion for Discovery at 2 n.3, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC) ("[T]o avoid disclosure of privileged information and simplify the Fourth Amendment analysis, the United States will concede, for purposes of any forthcoming motion to suppress, that the FBI located the aircard within Unit 1122 of the Domocilio Apartments."). With the "search" concession, the defendant is not harmed by any lack of disclosure — Rigmaiden gets to start from the position that the government's actions constituted a Fourth Amendment search and seizure and can then make all arguments that flow from that position, while the government can protect details that it believes could assist potential targets in evading detection by the technology in the future. *See* United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013

seeks to protect its use of cell site simulators as a sensitive source and method — to the extent that it will not even acknowledge the name of the specific equipment it uses[173] — is, however, consistent with a larger effort to prevent public disclosure of the technology and its capabilities. We address that effort next.

IV. THE GOVERNMENT'S SECRET STRINGRAY

Based on the recent public disclosure of an affidavit by Agent Bradley S. Morrison, the head of the FBI team responsible for the agency's use of StingRay and other cellular tracking technologies, we now know that the Rigmaiden prosecutors' efforts to shield details about the StingRay were part of a coordinated effort across federal, state, and local agencies to keep law enforcement use of this equipment secret.[174] Specifically, Agent Morrison asserts that "disclosure of what appears to be innocuous information about the use of cell site simulators would provide adversaries with critical information . . . necessary to develop defensive technology, modify their behaviors, and otherwise take countermeasures designed to thwart the use of this technology."[175] Agent Morrison warns that disclosure "could result in the FBI's inability to protect the public from terrorism and other criminal activity because, through public disclosures, this technology has been rendered essentially useless for future investigations."[176] Similar arguments have been made by a number of other local law enforcement agencies across the country.[177]

In order to ensure the continued effectiveness of cellular surveillance equipment, the FBI, for the past ten years, has taken significant

---

WL 1932800, at *4 (D. Ariz. May 8, 2013) (finding "that Defendant was fully able to make his Fourth Amendment arguments in light of the extensive disclosures provided by the government, detailed stipulations of fact agreed to by the government, and information Defendant was able to obtain through his own investigations" and that "Defendant has been placed at no disadvantage by the government's withholding of sensitive law enforcement information"). Moreover, because law enforcement can generally switch to carrier-assisted surveillance once a cell site simulator is used to identify a target, it is feasible to exclude the use of IMSI catcher technology from the government's case-in-chief trial evidence. In other words, because an IMSI catcher may only be initially necessary to identify or locate a target (which may not be relevant proof of the charges at trial), additional tracking of a target, when needed, can be performed with carrier-assisted surveillance, which can be used as evidence at trial without fear of exposing a sensitive source or method. Indeed, in the Rigmaiden prosecution, the court noted that "the government ha[d] never suggested that it intend[ed] to present evidence about its location of the aircard [i.e., data-card] at trial." United States v. Rigmaiden, 844 F. Supp. 2d 982, 989 (D. Ariz. 2012).

173. *See* Morrison Affidavit 2012, *supra* note 50, at 1.

174. Affidavit of FBI Supervisory Special Agent Bradley S. Morrison, Chief, Tracking Technology Unit, Operation Technology Division in Quantico Division, at 2, Apr. 11, 2014, attachment to City's Verified Answer, Hodai v. City of Tucson, No. C20141225 (Ariz. Supr. Ct. Apr. 14, 2014) [hereinafter Morrison Affidavit 2014].

175. *Id*. at 1–2.

176. *Id*. at 2.

177. *See* discussion *infra* Part IV.C.

steps to prevent the disclosure of information about the specific electronic equipment and techniques used by law enforcement.[178] These steps include what might be characterized as a purposeful lack of disclosure to magistrate judges when seeking approval to use a cell site simulator in a criminal investigation, strict non-disclosure agreements with state and local law enforcement, and essentially across-the-board refusals to turn over documents relating to cell site simulators in response to Freedom of Information Act ("FOIA") and public records requests. This Part describes the growth (one might even say the metastasis) of a discourse of secrecy regarding the StingRay's use across various channels and levels of government.

A. Lack of Disclosure to the Courts

Despite the fact that U.S. government agencies have used cellular surveillance devices for more than twenty years, the 2012 Judge Owsley opinion is one of only two known published magistrate opinions to address law enforcement use of this technology. There are several possible reasons for this dearth of judicial analysis,[179] but one of the most troubling possibilities may be a lack of knowledge on the part of magistrate judges about the specific surveillance technique(s) they are authorizing, due to a lack of candidly presented explanatory information in the government's applications. In one set of DOJ emails obtained by the American Civil Liberties Union ("ACLU") through a Freedom of Information Act request, for example, a federal prosecutor in Northern California noted that "many agents are still using [cellular surveillance technology with a] pen register application [that] does not make [the use of that technology] explicit."[180] Similarly, at a conference at Yale Law School in 2013, Judge Owsley indicated that federal agents may frequently obfuscate the planned use of a StingRay in authorization requests:

> "I may have seen them before and not realized what it was, because what they do is present an application that looks essentially like a pen register application . . . . So any magistrate judge that is typically looking at a lot of pen register applications and not

178. *Id*.

179. For a broader discussion of the reasons underlying the lack of judicial review of law enforcement use of the StingRay, see Pell & Soghoian, *supra* note 97.

180. E-mail from Miranda Kane, Chief, Criminal Div., U.S. Attorneys Office Northern District Cal., to USACAN-Attorneys-Criminal, U.S. Dep't of Justice (May 23, 2011, 11:55 PST), *available at* https://www.aclu.org/files/assets/doj_emails_on_stingray_requests.pdf.

> paying a lot of attention to the details may be signing an application that is authorizing a Sting[R]ay."[181]

In Tacoma, Washington, the local police have used StingRay surveillance devices since 2009 and insist that they only do so with approval from a judge.[182] When asked about the police department's statements in 2014, however, the presiding judge of the local Superior Court told a reporter that the StingRay equipment had not been mentioned in any warrant applications that he has seen. He also revealed that other judges in his court were similarly surprised to hear that the Tacoma police were using the technology, stating that "[the judges] had never heard of it."[183]

That prosecutors have not made this information clear to judges often appears to be an intentional action. In the Rigmaiden case, for example, prosecutors conceded that the government had not made a "full disclosure to the magistrate judge [who issued the original order authorizing the surveillance] with respect to the nature and operation of the [StingRay] device [used to locate Rigmaiden]."[184] The reason for that lack of candor, the DOJ later told the court, was "because of the sensitive nature of the device in terms of concerns out of the disclosure to third parties."[185]

Likewise, two notable events in Florida suggest an intentional effort by local law enforcement in that state to protect details about the use and functions of cellular surveillance technology. In a 2008 state case, police in Tallahassee used a StingRay to locate a victim's stolen phone in the defendant's apartment.[186] The police later revealed that they "did not want to obtain a search warrant because they did not

---

181. Ryan Gallagher, *Feds Accused of Hiding Information from Judges About Covert Cellphone Tracking Tool*, SLATE (Mar. 28, 2013), http://www.slate.com/blogs/future_tense/2013/03/28/stingray_surveillance_technology_used_without_proper_approval_report.html (quoting Judge Owsley); *see also* Jennifer Valentino-DeVries, *supra* note 26 (reporting that when a prosecutor was asked by the judge how a court order or warrant could be obtained without telling the judge what technology was being used, the prosecutor responded "[i]t was standard practice, your honor").

182. *See* Kate Martin, *Tacoma Police Admit to Cellphone Surveillance, Say They Don't Keep Data*, NEWS TRIB. (Aug. 27, 2014), http://www.thenewstribune.com/2014/08/27/3349396/tpd-responds-to-cell-phone-surveillance.html.

183. *See id*.

184. Transcript of Motion To Suppress at 81, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

185. *Id*. at 81–82. The DOJ prosecutor also told the court, "Obviously, if the magistrate judge had had questions, he would have been entitled to answers, as any magistrate judge." But when the court noted that it was "not the magistrate's burden to ferret that [information] out while he's got the agents in his office," the prosecutor conceded that it was not. *Id*.

186. *See* Thomas v. Florida, 127 So. 3d 658, 660 n.2 (Fla. Dist. Ct. App. 2013); Nathan Freed Wessler, *VICTORY: Judge Releases Information About Police Use of Stingray Cell Phone Trackers*, ACLU FREE FUTURE BLOG (June 3, 2014), https://www.aclu.org/blog/national-security-technology-and-liberty/victory-judge-releases-information-about-police-use (a transcript from the trial, unsealed at the ACLU's request, confirms that the police used a StingRay in the case).

want to reveal information about the technology they used to track the cell phone signal."[187] In addition, an investigator with the technical operations unit of the Tallahassee Police Department testified: "[W]e prefer that alternate legal methods be used, so that we do not have to rely upon the equipment to establish probable cause, [in order to avoid] reveal[ing] the nature [of the surveillance] and methods [used]."[188]

In Sarasota, police have enacted a policy of describing StingRay-derived intelligence in depositions and reports as "'information from a confidential source regarding the location of the suspect . . . .'"[189] According to emails obtained by the ACLU, this policy, which was requested by the U.S. Marshals, is intended to shield information about the StingRay "so that [law enforcement] may continue to utilize this technology without the knowledge of the criminal element."[190] Even if the aim of this policy is to keep the general public in the dark, by including misleading information in court documents, the police are also preventing the courts from having a true understanding of the electronic surveillance that is being conducted under their watch.

B. Secrecy via Regulatory Restrictions and Non-Disclosure Agreements

The Harris Corporation, which manufactures the StingRay, has submitted to the FCC applications for equipment-authorization licenses for each of its cellular-surveillance products.[191] These applications include language provided by the FBI,[192] which requests that the FCC impose specific conditions as part of regulatory agency's authorization of Harris' surveillance equipment:

---

187. *Thomas*, 127 So. 3d at 660.

188. *Id*.

189. *See* Joe Palazzolo, *Suspects in Florida Tracked by Cellphone "Stingray" Tool*, WALL ST. J. (June 20, 2014), http://online.wsj.com/articles/suspects-in-florida-tracked-by-cellphone-stingray-tool-1403302294.

190. *See* Kim Zetter, *Emails Show Feds Asking Florida Cops to Deceive Judges*, WIRED (June 19, 2014), http://www.wired.com/2014/06/feds-told-cops-to-deceive-courts-about-stingray/.

191. *See* Letter from Tania W. Hanna, Vice President of Legislative Affairs & Pub. Policy, Harris Corp., and Evan S. Morris, Counsel on Gov't Relations, Harris Corp., to Marlene H. Dortch, Sec'y, FCC (Apr. 28, 2011), *available at* http://files.cloudprivacy.net/Harris-FCC-confidential-request-1.pdf; Letter from Tania W. Hanna, Vice President of Legislative Affairs & Pub. Policy, Harris Corp., and Evan S. Morris, Counsel on Gov't Relations, Harris Corp., to Marlene H. Dortch, Sec'y, FCC (Mar. 21, 2011), *available at* http://files.cloudprivacy.net/Harris-FCC-confidential-request-2.pdf.

192. *See* E-mail from [redacted] to [redacted] (June 28, 2010, 10:56 EST), *available at* https://www.aclu.org/sites/default/files/assets/fcc_foia_harris_emails.pdf ("Harris has agreed with the [FBI] to request that the Commission condition its equipment authorization for the StingRay® product in order to address concerns over the proliferation of surreptitious law enforcement surveillance equipment.").

> (1) The marketing and sale of these devices shall be limited to federal/state/local public safety and law enforcement officials only; and
>
> (2) State and local law enforcement agencies must [in] advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization.[193]

The FCC submissions filed by Harris go on to explain that the purpose of the requested license restrictions is to ensure that use of the product be "limited to its intended use, operated only by federal, state, and local public safety officials" and to "address concerns regarding the proliferation of the equipment to unauthorized users."[194]

The FBI and DOJ are indeed coordinating the use of this technology, particularly through non-disclosure agreements, to limit disclosure to the public of information about cellular interception equipequipment. The FBI has entered into non-disclosure agreements with state and local enforcement partners.[195] The FBI argues that information shared by the federal government with states "concerning cell site simulator technology is considered homeland security information under the Homeland Security Act."[196] The result of this classification is that cell site simulator information "remain[s] under the control of the [FBI] . . . ."[197]

---

193. *See* Letter from Tania W. Hanna to Marlene H. Dortch (Apr. 28, 2011), *supra* note 191, at 2 (emphasis removed).

194. *Id*.

195. Morrison Affidavit 2014, *supra* note 174, at 2; *see also* Letter from Laura M. Laughlin, Special Agent in Charge, Seattle Div., Fed. Bureau of Investigation, to Donald Ramsdell, Chief of Police, Tacoma Police Dep't (Dec. 19, 2012), *available at* http://s3.documentcloud.org/documents/1303020/nda_redacted.pdf ("Consistent with the conditions on the equipment authorization granted to Harris Corporation by the [FCC], state and local law enforcement agencies must coordinate with the [FBI] to complete this non-disclosure agreement prior to the acquisition and use of the equipment/technology authorized by the FCC authorization."); Jennifer Portman, *FDLE Signed Stingray Non-Disclosure Deal*, TALLAHASSEE DEMOCRAT (Mar. 30, 2014), http://www.tallahassee.com/article/20140330/NEWS01/303300011/FDLE-signed-Stingray-non-disclosure-deal ("[The Florida Department of Law Enforcement] Commissioner Gerald Bailey said his agency had a non-disclosure agreement with the FBI to not reveal information about the technology . . . .").

196. *See* Morrison Affidavit 2014, *supra* note 174, at 3 (explaining that 6 U.S.C. §§ 482(f)(1)(B)–(D) "defines homeland security information as information that relates to the ability to prevent, interdict, or disrupt terrorist activity; information that would improve the identification or investigation of a suspected terrorist or terrorist organization; or information that would improve the response to a terrorist act," and asserting that "[c]ell site simulator technology meets all three criteria").

197. *Id*. (relying on 6 U.S.C. § 482(e), which states that homeland security information "obtained by a State or local government from a Federal agency under this section shall remain under the control of the Federal agency, and a State or law authorizing or requiring such a government to disclose information shall not apply to such information").

Local law enforcement agencies that have purchased Harris cellular interception technology have also signed non-disclosure agreements with the manufacturer of the equipment. The Harris non-disclosure agreement, which has been obtained by activists through Open Records Act requests,[198] specifically prohibits the disclosure of any information about the use of the company's products, including operations, missions, and investigative results that would be deemed a "release of technical data . . . ."[199]

C. Federal FOIA and State Public Records Act Responses

Over the past few years, privacy advocates and journalists have submitted numerous open records requests to federal and state law enforcement agencies seeking any documents pertaining to StingRays and related surveillance technologies.[200] The FBI, DOJ, and Department of Homeland Security ("DHS") have, collectively, located more than 24,000 pages of relevant documents, but have either withheld them in their entirety or released them in such a heavily redacted form that they reveal little to no useful information.[201]

To justify their limited disclosure, the FBI, DOJ, and DHS claim a number of FOIA exemptions, including arguments that the production of documents would: (1) reveal classified information;

198. *See* Kim Zetter, *Police Contract with Spy Tool Maker Prohibits Talking About Device's Use*, WIRED (Mar. 4, 2014), http://www.wired.com/2014/03/harris-stingray-nda/.

199. *See* Complaint for Statutory Special Action & Injunctive Relief & Application for Order to Show Cause at Ex. B, Hodai v. City of Tucson, No. 14-1225 (Ariz. Super. Ct. Mar. 3, 2014), *available at* http://www.wired.com/images_blogs/threatlevel/2014/03/ACLU-Stingray-Complaint-Hodai-v-TPD.pdf.

200. *See EPIC v. FBI — Stingray / Cell Site Simulator*, ELEC. PRIVACY INFO. CTR., https://epic.org/foia/fbi/stingray/ (last visited Dec. 18, 2014) (collecting documents released by DOJ relating to FBI's use of cell site simulators); Nathan Freed Wessler, *Police Hide Use of Cell Phone Tracker from Courts Because Manufacturer Asked*, ACLU FREE FUTURE BLOG (Mar. 3, 2014), https://www.aclu.org/blog/national-security-technology-and-liberty/police-hide-use-cell-phone-tracker-courts-because (reporting that "the ACLU and ACLU of Florida have teamed up . . . submitting public records requests to nearly 30 police and sheriffs' departments across Florida seeking information about their acquisition and use of [S]ting[R]ays").

201. *See* Letter from Kenneth Courter, Acting Chief, FOIA/PA Unit, Criminal Div., U.S. Dep't of Justice, to author, at 1 (July 17, 2013), *available at* http://files.cloudprivacy.net/DOJ-Stingray-FOIA-5th-reply.pdf ("As to the portion of your request for information concerning cell site simulators, digital analyzers, and similar mobile phone surveillance technology generally, the Criminal Division processed an additional five hundred and sixty-seven pages of responsive records, and has determined that these records are exempt from disclosure . . . ."); Letter from Tony R. Tucker, FOIA Officer, Office of Intelligence and Analysis, U.S. Dep't of Homeland Sec., to author, at 2 (Feb. 17, 2012), *available at* http://files.cloudprivacy.net/DHS-OIA-Stingray-FOIA-reply.pdf ("[T]he Office of Intelligence and Analysis located 1085 pages. Of these total pages, 1046 must be withheld in their entirety . . . ."); Fourth Decl. of David M. Hardy at 9, EPIC v. FBI, No. 12-0667 (D.D.C. Oct. 1, 2013), *available at* https://epic.org/foia/fbi/stingray/Fourth-Hardy-Declaration.pdf ("The FBI reviewed and processed a total of 22,982 pages of responsive material, of which, 4,377 pages were released in full or in part, and 18,605 were withheld in full.").

(2) disclose techniques and procedures for law enforcement investigation; and (3) reasonably be expected to risk circumvention of the law.[202]

Consistent with the government's FOIA positions, the prosecutor in the Rigmaiden case stated that "the sensitive nature of the equipment [used to locate the defendant] goes beyond issues of law enforcement to matters of national security," as "some of this equipment is not only used in the law enforcement realm, it's used in the national security realm."[203]

Local law enforcement agencies have similarly been evasive. In response to queries from journalists working with USA Today, thirty-six police agencies refused to confirm whether or not they have even used cellular surveillance equipment.[204] Several state and local law enforcement agencies have also refused to disclose records related to the use of this technology, arguing that "criminals or terrorists could use the information to thwart important crime-fighting and surveillance techniques."[205] In sum, these federal and state responses, while perhaps lawful responses to FOIA and Public Records Act requests, illustrate a much larger secrecy policy and narrative: Law enforcement agencies believe that the existence, capabilities, and limitations of this cellular interception technology are secret and that the secrecy must persist in order for the technology to continue to be an effective law enforcement surveillance tool.[206]

V. A SECRET NO MORE

While U.S. government agencies shroud cellular surveillance technology in secrecy, in several other countries this same technology is subject to legislative oversight, judicial review, and, thus, public discourse. In still other countries, the unregulated nature of this technology has led to a chaotic situation where thousands of untracked

---

202. *See* Letter from Kenneth Courter to author, *supra* note 201, at 2; Letter from Tony R. Tucker to author, *supra* 201, at 1; Decl. of Hardy, *supra* note 201, at 12.

203. Status Conference, Reporter's Partial Tr. of Proceedings at 14, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC).

204. *See* Kelly, *supra* note 21.

205. *Id*.

206. *See* Taylor Killough, *State Police Acknowledge Use of Cell Phone Tracking Device*, IND. PUB. MEDIA (Dec. 12, 2013), http://indianapublicmedia.org/news/state-police-respond-investigation-tracking-device-59918/ ("Indiana State Police Captain Dave Bursten said in a statement the department is working well within the bounds of the law . . . . Bursten won't say exactly how the [StingRay] technology is used, because he says it would be 'like a football team giving up their playbook.'"); Nathan Freed Wessler, *Local Police in Florida Acting Like They're the CIA (But They're Not)*, ACLU FREE FUTURE BLOG (Mar. 25, 2014), https://www.aclu.org/blog/national-security-technology-and-liberty/local-police-florida-acting-theyre-cia-theyre-not (describing a "Glomar" response from the Sunrise, Florida Police Department, neither confirming nor denying the existence of documents related to the purchase of Harris cellular surveillance technology).

interception devices are in use, many by non-governmental actors. Moreover, skilled hobbyists using readily available off-the-shelf components can now build homemade cellular interception devices for a tiny fraction of the cost law enforcement and security agencies pay for Harris' StingRay. In detailing the existence of an open, global market for cellular interception technology, this Part dispels any rational notion that cellular interception technology is or can be kept secret.

A. The Globalization of Cellular Interception Technology

The first generation of cellular interception technology was introduced during the early-1990s.[207] Generally, it was expensive and sold by a few defense contractors only to major global powers. Today, however, both passive and active surveillance devices are much cheaper and available on the open market from surveillance vendors in the Middle East, South America, and Asia.[208] The major powers thus no longer enjoy a monopoly over cellular phone surveillance. It has become, for better or for worse, irreversibly globalized.

Defense contractors sold the first phone interception devices to world powers such as Germany,[209] the United Kingdom,[210] the United States,[211] and most likely, Russia and Israel.[212] Over the past three decades, the market for this technology has steadily expanded and the price of the technology has, consequently, dropped.[213] Manufacturers

---

207. *See supra* Part II.A.

208. *See infra* notes 214–221.

209. *Cf*. *supra* notes 59–60.

210. *Cf*. MMI Research Ltd v. Cellxion Ltd & Ors, [2009] EWHC (Pat) 418, [78] (Eng.), *available at* http://www.bailii.org/ew/cases/EWHC/Patents/2009/418.html (describing the demonstration of the GSM-X interception device to potential government clients in 1999 by MMI Research Ltd, a British surveillance equipment manufacturer).

211. *See supra* Part II.A.

212. Given the active, sophisticated espionage efforts of the Russian and Israeli intelligence agencies, it is almost certainly the case that companies in these countries were early manufacturers of this technology too. Today, there are many large companies in Israel and Russia that actively export cellular surveillance equipment around the world. For Israel, see *Cellular Interception*, ABILITY COMPUTERS & SOFTWARE INDUS. LTD., http://www.interceptors.com/intercept-solutions/Cellular-Interception.html (last visited Dec. 18, 2014); *Septier Guardian Tactical Systems*, SEPTIER COMMC'N LTD., http://www.septier.com/93.html (last visited Dec. 18, 2014) (describing several cellular surveillance products). For Russia, see Andrei Soldatov & Irina Borogan, *5 Russian-Made Surveillance Technologies Used in the West*, WIRED: DANGER ROOM (May 10, 2013), http://www.wired.com/dangerroom/2013/05/russian-surveillance-technologies (The Discovery Telecom Technologies system "masquerades as a cell phone tower, sucking in nearby signals and allowing the device's operator to surreptitiously listen and record. Established in Moscow, the firm . . . boasts on its Russian website about including the Kremlin and the FSB among its clients.").

213. *Compare* Kelly, *supra* note 21 ("The cell-tracking systems [purchased by U.S. law enforcement agencies] cost as much as $400,000, depending on when they were bought and what add-ons they have. The latest upgrade, code-named 'Hailstorm,' is spurring a wave of upgrade requests."), *with* Letter from Alan M. Grayson to Tom Wheeler, *supra* note 29

and resellers now include firms in Argentina,[214] Bangladesh,[215] Canada,[216] China[217], India,[218] Malaysia,[219] the Netherlands,[220] Pakistan,[221] Switzerland,[222] Taiwan,[223] and Turkey,[224] who, in addition to selling devices to their own governments, actively seek out other government (and, perhaps, non-government) customers as part of the five-billion dollar global market for commercial surveillance technology.[225] Indeed, cellular interception devices are reportedly among the "bestselling items" exhibited at surveillance industry trade shows.[226]

Although several governments have employed phone interception technology, the extent to which it has been used responsibly and disclosed to the public varies considerably by country. Germany is perhaps the most open and transparent country regarding its use of active interception technology. The use of such devices by German govern-

---

(citing one online merchant in China, "IMSI catchers can apparently 'be bought openly' from online retailers for as little as $1800").

214. *See Products*, SOLUCIONES-PARA-GOBIERNO.COM, http://solucionesparagobierno.com/english/productos.html (last visited Dec. 18, 2014).

215. *Passive GSM (Dual Band) / CDMA Monitoring System*, ALIBABA.COM, http://www.alibaba.com/product-detail/Passive-GSM-Dual-Band-CDMA-Monitoring_103809673.html (last visited Oct. 7, 2014).

216. *GSS Pro-A GSM Interceptor*, GLOBAL SEC. SOLUTIONS, http://www.global-security-solutions.com/ProAInterceptor.html (last visited Dec. 18, 2014).

217. *See* Letter from Alan M. Grayson to Tom Wheeler, *supra* note 29.

218. *See Cellular Monitoring*, SHOGHI COMMC'NS LTD., http://www.shoghicom.com/cellular-monitoring.php (last visited Dec. 18, 2014) (describing the cellular intercept products available for sale); *IMSI Catcher*, TRADEIM.COM, http://www.tradeim.com/company.html?method=product&productCode=8693695 (last visited Dec. 18, 2014).

219. *See GSM Interceptor*, INFRALANGIT, http://infralangit.com/gsm-interceptor/ (last visited Oct. 7, 2014).

220. *See GSM Interception System*, PI PRODUCTS, http://www.pi-products.nl/pi-products/PDF/Communication%20Monitoring/Monitoring%20GSM%20networks/gsm%20interception%20system.pdf (last visited Dec. 18, 2014).

221. *See GSM Interceptor Scanner*, WEIKU.COM, http://www.weiku.com/products/18444632/GSM_interceptor_Scanner.html (last visited Dec. 18, 2014).

222. *See Catalogue*, NEOSOFT AG, https://www.documentcloud.org/documents/810502-945-neosoft-catalogue.html (last visited Dec. 18, 2014).

223. *See IMSI Catcher*, ALIBABA.COM, http://www.alibaba.com/product-detail/IMSI-catcher_135958750.html (last visited Dec. 18, 2014) (listing the PKI 1640 for $1800 per unit, which can "catch all active UMTS mobile phones in your proximity" and capture and store date "such as IMSI, IMEI, TMSI").

224. *See Interceptor GSM A5-1 A5-2 ve 3*, ALIBABA.COM, http://www.alibaba.com/product-free/126383443/interceptor_gsm_A5_1_A5_2.html (last visited Dec. 18, 2014).

225. *See* Nicole Perlroth, *Software Meant To Fight Crime Is Used To Spy on Dissidents*, N.Y. TIMES (Aug. 30, 2012), http://www.nytimes.com/2012/08/31/technology/finspy-software-is-tracking-political-dissidents.html ("The market for such technologies has grown to $5 billion a year from 'nothing 10 years ago,' said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveillance show . . . .").

226. *See* Stefan Krempl, *28C3: New Attacks on GSM Mobiles and Security Measures Shown*, H OPEN (Dec. 28, 2011), http://www.h-online.com/open/news/item/28C3-New-attacks-on-GSM-mobiles-and-security-measures-shown-1401668.html (noting that Karsten Nohl of Security Research Labs reported, after a trip to the ISS trade fair, "that the bestselling items in the espionage community at present are devices for monitoring mobile phones, such as IMSI catchers").

ment agencies is specifically regulated by several statutes,[227] which mandate, among other things, that statistical data describing their use be aggregated and published by the German Parliament.[228] Moreover, there have been several formal parliamentary answers to questions submitted by the public regarding the use of IMSI catchers,[229] as well as a decision from the German Constitutional Court permitting their use.[230]

The way cellular interception devices are regulated in Norway is also noteworthy because of the degree to which the legislation permitting their use explicitly acknowledges the dragnet nature of the technology. The relevant law permits temporary mass monitoring of all calls in a specific area during which police listen to all phone calls in the suspect's community, regardless of whether the intercepted parties have any connection with the case under investigation.[231]

It is in India, however, where cell phone interception technology has had the most high profile and politically destabilizing impact. Beginning in 2005, agencies in the Indian national government imported passive cellular interception systems.[232] In 2010, audio recordings and

---

227. *See* Bundesverfassungsschutzgesetz [BVerfSchG] [Federal Constitution Protection Act], Dec. 20, 1990, as amended, BGBL. I at 2499, § 9, para. 4 (Ger.), *available at* http://www.gesetze-im-internet.de/bverfschg/__9.html. *See generally* MARKUS RAU, TERRORISM AS A CHALLENGE FOR NATIONAL AND INTERNATIONAL SECURITY: SECURITY VS. LIBERTY? 311 (Christian Walter et al. eds., 2004).

228. *See* DEUTSCHER BUNDESTAG DRUCKSACHEN, Bericht, Mar. 14, 2013, BT 17/12774 (Ger.) (2011 data), *available at* http://dip21.bundestag.de/dip21/btd/17/127/1712774.pdf; DEUTSCHER BUNDESTAG DRUCKSACHEN, Bericht, Feb. 10, 2012, BT 17/8638 (Ger.) (2010 data), *available at* http://dipbt.bundestag.de/dip21/btd/17/086/1708638.pdf.

229. *See* DEUTSCHER BUNDESTAG DRUCKSACHEN, Antwort, Sep. 10, 2001, BT 14/6885 (Ger.) (2001 response), *available at* http://dip21.bundestag.de/dip21/btd/14/068/1406885.pdf; DEUTSCHER BUNDESTAG DRUCKSACHEN, Antwort, Nov. 9, 2011, BT 17/7652 (Ger.) (2011 response), *available at* http://dipbt.bundestag.de/dip21/btd/17/076/1707652.pdf.

230. *See* Bundesverfassungsgerict [BVerfG] [Federal Constitutional Court] Aug. 22, 2006, ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICTS [BVERFGE] 2 BVR 1345/03 (Ger.), *available at* http://www.bundesverfassungsgericht.de/entscheidungen/rk20060822_2bvr134503.html; EURO. COMMISSION ANN. REP. OF ART. 29 WORKING PARTY ON DATA PROTECTION at 45–46 (2006), *available at* http://www.akvorrat.at/sites/default/files/VDS_Materialien/Art%2029%20WP%2010th_annual_report_en.pdf (English language summary of the ruling by the Federal Constitutional Court on 22 August 2006 on the use of the IMSI-catchers in criminal proceedings).

231. *See* Justis- og beredskapsdepartementet, *Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)* [*On Amendments to the Criminal Procedure Act and the Police Act (covert audio surveillance and the use of coercive measures to prevent serious crime)*], Ot.prp. nr. 60 (2004–2005) (Nor.), *available at* https://www.regjeringen.no/nb/dokumenter/otprp-nr-60-2004-2005-/id398192/?docId=OTP200420050060000DDDEPIS&q=&navchap=1&ch=8#KAP8-5-3; Per Anders Johansen, *Politiet og Forsvaret kan ta kontroll over mobilnettet* [*The Police and the Military to Take Control of Cellular*], AFTENPOSTEN (Sept. 21, 2014), http://www.aftenposten.no/nyheter/iriks/Politiet-og-Forsvaret-kan-ta-kontroll-over-mobilnettet-7713131.html.

232. Saikat Datta, *A Fox on a Fishing Expedition*, OUTLOOK INDIA (May 3, 2010), http://www.outlookindia.com/article.aspx?265192 ("India began purchasing the off-the-air

written transcripts of politicians' calls that were intercepted with these devices were leaked to the press, leading to a huge scandal.[233] Media reports revealed that, just two years after the devices were first purchased by the national intelligence agency, they were used to monitor the phone calls of senior politicians, including opposition leaders.[234]

An anonymous intelligence official told one Indian newspaper that cellular interception technology enabled them to "dig into everyone's life . . . be it political and corporate leaders, journalists, social activists or bureaucrats. We can track anyone we choose."[235] Another anonymous official stressed that the principal strategic advantage of the technology is that it:

> "works on deniability . . . . It can be deployed anywhere. We don't need to show any [formal legal] authorisation [sic] since we're not tapping a phone number at the [wireless carrier's office] but intercepting signals between the phone and the cellphone tower . . . . [W]e can [always] . . . erase the conversation. No one gets to know."[236]

In addition to the high-profile use of the devices against politicians, news reports also reveal that the equipment has been used to spy on business leaders, journalists, and families of politicians.[237] One intelligence official stated that "the [surveillance] machine intercepted calls of the wives of [members of parliament] discussing personal and sensitive matters, corporate leaders seeking private liaisons in hotels . . . . Most of the corporate calls at night are for sex."[238] Given the

---

GSM/CDMA monitoring systems around 2005–06, and the first interception of a mobile phone conversation using the system was carried out by the NTRO on January 7, 2006, in New Delhi."); Harish Gupta & Nivedita Mookerji, *Private Hand in Phone Tapping Worries Manmohan Singh; Probe Ordered*, DNA INDIA (Dec. 14, 2010), http://www.dnaindia.com/india/1481036/report-private-hand-in-phone-tapping-worries-manmohan-singh-probe-ordered ("These machines were first introduced in the NTRO, a top government technical surveillance agency directly under the PM, sometime in 2005.").

233. *See* Saikat Datta, *Bootleg Tapes: The Rulers Who Listen*, OUTLOOK INDIA (May 10, 2010), http://www.outlookindia.com/story.aspx?sid=4&aid=265272 (describing various conversations recorded using the surveillance technology and provided to the press).

234. Saikat Datta, *We, The Eavesdropped*, OUTLOOK INDIA (May 3, 2010), http://www.outlookindia.com/article.aspx?265191 (describing NTRO's interception of conversations of various politicians).

235. Datta, *supra* note 232 (internal quotation marks omitted).

236. Datta, *supra* note 234.

237. *See "Give Us Legal Immunity, We'd Be Happy To Provide Proof of Illegal Tapping,"* OUTLOOK INDIA (May 10, 2012), http://www.outlookindia.com/article/Give-Us-Legal-Immunity-Wed-Be-Happy-To-Provide-Proof-Of-Illegal-Tapping/265273 (interview with several anonymous senior intelligence officials confirming that "the machine records lots and lots of calls of ministers, MPs, bureaucrats, lobbyists, arms dealers, editors and journalists").

238. *Id*.

sensitive nature of the communications intercepted using these devices, another official described the problem in economic terms: "When an officer on a salary of [130 dollars] a month has pretty much unrestricted access to this kind of technology . . . things will go wrong, and have gone wrong."[239]

A subsequent official investigation revealed that lax customs rules permitted unregulated importation and purchase of the interception technology. Government officials later acknowledged that over forty different makes and models of cellular interception technology had been imported from over a dozen vendors.[240] The devices had been purchased by numerous national governmental agencies, state governments,[241] and the military.[242] Officials estimate that thousands of cellular interception devices have been imported,[243] and that hundreds are in the possession of private parties, such as corporations and detective agencies.[244]

By late 2010, senior Indian government officials acknowledged that legal prohibitions on the private purchase and use of cellular in-

---

239. Praveen Swami, *The Government's Listening to Us*, HINDU (Dec. 1, 2011), http://www.thehindu.com/news/national/the-governments-listening-to-us/article2678501.ece (internal quotation marks omitted).

240. Sudhi Ranjan Sen, *Phone-Tapping: Telecom Firms Under Scanner for Eavesdropping?*, NDTV (Sept. 25, 2012), http://www.ndtv.com/article/india/phone-tapping-telecom-firms-under-scanner-for-eavesdropping-271661 ("But the bad news is, of the 45-odd suspected machines identified, the government doesn't have the address of importers of as many as 24 machines."); Sanjay Singh, *Government Hunts for Elusive Bug: DoT Wants Snooping and Listening Devices Within Private Sector Surrendered*, DAILY MAIL (Nov. 27, 2012), http://www.dailymail.co.uk/indiahome/indianews/article-2239422/Government-hunts-elusive-bug-DoT-wants-snooping-listening-devices-private-sector-surrendered.html ("Despite the ban on the free import of phone interceptors, these gadgets manufactured in Israel, the UK, France and China continue to be smuggled into the country through Nepal and Bangladesh. It is believed that there [are] as many as 45 different variants of these machines . . . floating around in India.").

241. *See* Hitender Rao, *"Off-Air" Tapping: MHA Wants States To Surrender Devices*, HINDUSTAN TIMES (June 29, 2011), http://www.hindustantimes.com/Punjab/Chandigarh/Off-air-tapping-MHA-wants-states-to-surrender-devices/Article1-715297.aspx (describing their use by Haryana state government).

242. Ritu Sarin, *MHA Poses Fresh Queries About Army Interceptors*, INDIAN EXPRESS (Nov. 4, 2012), http://www.indianexpress.com/news/mha-poses-fresh-queries-about-army-interceptors/1026444/ (describing the home ministry's audit of army's deployment of off-air interception equipment).

243. *"Invisible" Phone Taps: Is the Govt Worried?*, NDTV (Mar. 2, 2012), http://www.ndtv.com/article/india/invisible-phone-taps-is-the-govt-worried-181763 ("'My inquiries with the government authorities have revealed that during the last three years, 1100 GSM monitoring interceptors were imported' . . . ."); Ritu Sarin, *States Begin To Surrender Off-Air Phone Snooping Equipment*, FIN. EXPRESS (June 5, 2012), http://www.financialexpress.com/news/states-begin-to-surrender-offair-phone-snooping-equipment/957859 (stating that as many as 73,000 dual-use devices had been imported, and some could be employed for innocuous purposes).

244. Singh, *supra* note 240 (estimating that, between the government and private sector, 2000 off-air surveillance devices imported in 2000); *"Invisible" Phone Taps*, *supra* note 243 ("Sources in the Telecom Department and Home Ministry suspect that among the buyers are large corporate houses, politically-aligned detective agencies and even government agencies who are not authorised to carry out cellphone taps.").

terception technology would not protect the privacy of citizens' communications. India's prime minister stressed the need to "look for solutions through technology to prevent access of telephone conversations . . . ."[245] Another senior government official acknowledged that the secrecy of government communications was threatened by the private use of interception technology.[246]

B. The Democratization of Cellular Interception Technology

The effective monopoly over cellular interception technology long enjoyed by governments was largely due to the cost.[247] Devices retail for as much as $400,000,[248] depending on the features — far too expensive for the average person, but a relatively small sum for the military, intelligence community, and even many law enforcement agencies. Part of the high price reflected the difficulty and significant capital investment required to design and manufacture the StingRay's sophisticated radio equipment. As a result, hobbyists and researchers without large budgets were simply unable to develop cellular communications technology. This cost barrier no longer exists. Moreover, a set of free software tools has been developed by a community of researchers and hobbyists that has lowered the skill level necessary to tinker with cellular communication technology. Consequently, as the cost and ease of developing cellular interception technology has declined, the longstanding nation-state monopoly has vanished. Surveillance has become democratized and, correspondingly, the motives for surveillance have multiplied. The next elements of this Part will describe briefly how innovations in radio technology have enabled researchers and hobbyists without large budgets to develop their own cellular interception devices.

---

245. Manoj Mitta, *Off-the-Air Taps a Bigger Worry: PM*, TIMES OF INDIA (Dec. 15, 2010), http://articles.timesofindia.indiatimes.com/2010-12-15/india/28230420_1_cabinet-secretary-telephone-interception-national-technical-research-organization (internal quotation marks omitted).

246. Singh, *supra* 240 ("A[n] [anonymous] top government official . . . said a large number of corporate houses have small offices in and around central Delhi areas in the proximity of important government buildings. 'Officials working in key positions under various ministries and sensitive departments are, therefore, vulnerable to phone tapping . . . .'").

247. *See* Ralf-Philipp Weinmann, *Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular Protocol Stacks*, 6TH USENIX WORKSHOP ON OFFENSIVE TECHNOLOGIES (Aug. 6, 2012), https://www.usenix.org/system/files/conference/woot12/woot12-final24.pdf ("In the past, spoofing a GSM network required a significant investment, which limited the set of possible attackers . . . . Open-source solutions such as OpenBTS allow anyone to run their own GSM network at a fraction of the cost of carrier-grade equipment, using a simple and cheap software-defined radio.").

248. Kelly, *supra* note 21 ("The cell-tracking systems cost as much as $400,000, depending on when they were bought and what add-ons they have. The latest upgrade, code-named 'Hailstorm,' is spurring a wave of upgrade requests.").

1. Low Cost Software-Defined Radio-Based Active Interception

Hobbyists can now build their own active surveillance devices with readily available electronic components currently costing approximately $700.[249] The ability to create such low-cost cellular interception devices is due to technological innovations that have lowered both the costs and skill-level necessary to develop radio technology. Specifically, a revolution in *software-defined radio* technology during the past decade has eliminated the longstanding technical barriers that prevented researchers and hobbyists from being able to experiment freely with large swaths of the radio spectrum. Software-defined radios are flexible hardware platforms that, when combined with specific software, "can change the frequency range, modulation type or output power of a radio device without making changes to hardware components."[250] Instead of having to create expensive new microchips (i.e., *hardware*) for each new radio technology — such as GPS navigation, Bluetooth, and High Definition TV — a low cost software-defined radio, combined with specific software for a particular application, can now be used instead.

The development of software-defined radio has reduced earlier barriers of access to radio technology, thus enabling tinkering by researchers of varied skill-levels. This access has allowed developers to create, for example, free software capable of operating a cellular network. Indeed, OpenBTS is a popular open source, cellular base station software suite,[251] which is designed to work with low cost (currently around $700) software-defined radios.[252] The existence of OpenBTS and similar software has thus significantly reduced the cost of creating and running a cellular network and brought it within the reach of non-profit organizations, rural communities, and hobbyists.[253]

---

249. Taylor Killian, *SDR Showdown: HackRF vs. bladeRF vs. USRP*, TAYLOR KILLIAN (Aug. 7, 2013), http://www.taylorkillian.com/2013/08/sdr-showdown-hackrf-vs-bladerf-vs-usrp.html (describing a specifications for a number of hobby radios ranging in price from $300 to $1100).

250. *See* Press Release, Federal Commc'ns Comm'n, FCC Approves First Software Defined Radio (Nov. 19, 2004), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-254463A1.pdf.

251. *See id*.; Harvind Samra, *The OpenBTS Project — An Open-Source GSM Base Station*, LWN.NET (Sept. 4, 2008), http://lwn.net/Articles/296949/.

252. *See generally* Killian, *supra* note 249 (comparing various software-defined radios).

253. Volunteers using OpenBTS have operated free cellular networks at Burning Man, a popular festival held in the Nevada desert, as well as at several computer security conferences. *See* Davis Burgess, *Burning Man 2011 — Yes We Were There*., OPENBTS CHRONICLES (Sept. 6, 2011), http://openbts.blogspot.com/2011/09/burning-man-2011-yes-we-were-there.html; Dan Goodin, *At DEFCON, Hackers Get Their Own Private Cell Network: Ninja Tel*, ARS TECHNICA (July 28, 2012), http://arstechnica.com/security/2012/07/ninja-tel-hacker-phone-network/. Non-profit organizations have also used OpenBTS to provide cellular service to remote communities in developing countries. *See* Stephen Lawson, *Cell System Used in Antarctica May Help To Cover the Plains*, COMPUTERWORLD (Mar. 26, 2013), http://www.computerworld.com.au/article/457350/

Once hobbyists and researchers were able to build and operate their own cellular networks with open source software, it was only a matter of time before the software was modified such that it could masquerade as a legitimate wireless carrier's network with the capacity to intercept calls.[254] Indeed, a security researcher did just that in 2010 — in front of an audience at the DEF CON security conference — using a laptop running OpenBTS that had been configured to masquerade as AT&T's network, thereby allowing the researcher to intercept outgoing calls from the phones of audience members.[255] Although the hardware and software necessary to build an OpenBTS-based cellular interception device is readily available, doing so still takes a significant amount of technical expertise. As is often the case with difficult-to-exploit security vulnerabilities, however, the usability barriers eventually shrink with the development of easy-to-use software.[256] Once these usability barriers are removed, low-cost interception tools will be available to anyone with a motive or interest in listening to the calls of others.[257]

---

cell_system_used_antarctica_may_help_cover_plains/ ("One [OpenBTS] network[] serves a remote village in Papua, Indonesia, that can only reach the outside world via satellite. Residents of the village can now call and text each other and exchange text messages with the rest of the world using an OpenBTS network linked to a satellite transceiver."); Jacqueline Mpala & Gertjan van Stam, *Open BTS, a GSM Experiment in Rural Zambia*, AFRICOMM 2012: FOURTH INTERNATIONAL IEEE EAI CONFERENCE ON E-INFRASTRUCTURE AND E-SERVICES FOR DEVELOPING COUNTRIES (Nov. 2012), http://www.academia.edu/2122498/Open_BTS_a_GSM_experiment_in_rural_Zambia.

254. David Burgess, the co-creator of OpenBTS who has previously written software for commercial IMSI catchers has observed, "Nearly any BTS or BTS simulator can be used as the basis of an IMSI-catcher." David Burgess, *Some Comments on IMSI-Catchers*, OPENBTS CHRONICLES (May 6, 2009), http://openbts.blogspot.com/2009/04/some-comments-on-imsi-catchers.html.

255. DEFCONConference, *DEF CON 18 — Chris Paget — Practical Cellphone Spying* at 23:36, YOUTUBE (Nov. 8, 2013), https://www.youtube.com/watch?v=fQSu9cBaojc (recording of Chris Paget's talk at DEF CON 18 on July 31, 2010).

256. *See* Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1399 (2008) ("[S]ometimes Superusers empower ordinary users with easy-to-use [hacking] software."); Kate Murphy, *New Hacking Tools Pose Bigger Threats to Wi-Fi Users*, N.Y. TIMES, Feb. 17, 2011, at B8, *available at* http://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html ("Until recently, only determined and knowledgeable hackers . . . could spy while you used your laptop or smartphone at Wi-Fi hot spots. But a free program called Firesheep . . . has made it simple to see what other users of an unsecured Wi-Fi network are doing and then [impersonate] them [on] sites they visited.").

257. For example, one German graduate student created a more usable IMSI catcher based on OpenBTS for his master's thesis. *See* Dennis Wehrle, Open Source IMSI-Catcher (Oct. 28, 2009) (unpublished Masters thesis, University of Freiburg), *available at* https://github.com/tom-mayer/imsi-catcher-detection/blob/master/Papers/Thesis%20KS/Ausarbeitung-Dennis_Wehrle.pdf.

2. Lower Cost Active Interception with Femtocells

Technically skilled hobbyists and researchers can create even cheaper, more organic active interception technology using a "femtocell," a device that extends the carrier's own network. Wireless providers have augmented their networks with devices known as microcells, picocells, and femtocells to provide better cellular service to their customers and to fill in "dead spots" where there is poor reception.[258] These small cellular base stations, which customers can install in their homes or offices, provide cellular connectivity to nearby phones within tens or hundreds of meters.[259] Indeed, these devices are already widely deployed in the U.S. — Sprint and AT&T each have distributed more than 1 million femtocells.[260]

From the perspective of a cellular phone, a femtocell is a normal cellular base station, indistinguishable from a carrier's base station installed at a cell tower. Because they must be installed in consumers' homes, the devices, unlike traditional cell towers, are small, easy to use, and inexpensive. They are typically sold for less than $100[261] and often given away for free to consumers who complain about poor service.[262] The femtocell was, therefore, a naturally attractive target for security researchers.[263] The devices are widely available, affordable,

---

258. Microcells, picocells, and femtocells all employ the same underlying technology. The difference between these products is their effective range. Microcells, picocells, and femtocells provide service to areas of 200m–2km, 4m–200m, and 10m, respectively. *See* Dimitris Mavrakis, *Do We Really Need Femto Cells?*, VISIONMOBILE (Dec. 1, 2007), http://www.visionmobile.com/blog/2007/12/do-we-really-need-femto-cells/.

259. *See id*.

260. INFORMA TELECOMS & MEDIA, SMALL CELL MARKET STATUS 3 (Feb. 2013) ("Sprint's deployment reached 1 million units as of October 2012 and analysts estimate that AT&T's deployment has reached similar numbers."); Sue Marek, *Sprint's Femtocell Tally Tops 1M*, FIERCEWIRELESS (Oct. 24, 2012), http://www.fiercewireless.com/story/sprints-femtocell-tally-tops-1m/2012-10-24.

261. *See* Roger Cheng, *A Cell Tower of Your Very Own*, WALL ST. J. (July 8, 2010), http://online.wsj.com/article/SB10001424052748703636404575353153350315146.html ("AT&T has been rolling out the 3G Microcell, which provides a full signal to a surrounding area of up to 5,000 square feet, as an answer for customers in areas with poor reception. The price is $149.99. Verizon Wireless's femtocell, the 'Network Extender,' is priced at $99.99 . . . .").

262. *See* Eric Savitz, *Sprint Giving Femtocells to Some Customers; Will VZ, T Follow?*, BARRON'S (Sept. 15, 2010), http://blogs.barrons.com/techtraderdaily/2010/09/15/sprint-giving-femtocells-to-some-customers-will-vz-t-follow/.

263. *See generally* Ravishankar Borgaonkar, Kevin Redon & Jean-Pierre Seifert, *Security Analysis of a Femtocell Device*, *in* PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON SECURITY OF INFORMATION AND NETWORKS 95–102 (Nov. 14–19, 2011); Nico Golde, Kevin Redon & Ravishankar Borgaonkar, *Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication*, *in* PROCEEDINGS OF THE 19TH ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM (Feb. 2012); David Malone, Darren F. Kavanagh & Niall R. Murphy, *Rogue Femtocell Owners: How Mallory Can Monitor My Devices*, 5TH IEEE INTERNATIONAL TRAFFIC MONITORING AND ANALYSIS WORKSHOP (Apr. 19, 2013); *The Vodafone Access Gateway / UMTS FemtoCell / Vodafone Sure Signal*, THE HACKER'S CHOICE WIKI (July 13, 2011), http://wiki.thc.org/vodafone.

and fully functional as cellular base stations with the capability to deliver (and intercept) calls, text messages, and data connections. Moreover, the femtocells — like any computer — have security flaws that researchers have been able to exploit to gain administrative access. Indeed, researchers have then been able to modify the devices, turning the femtocells into hundred dollar surveillance devices capable of intercepting communications to and from nearby phones.[264] While the degree of technical skill necessary to turn a femtocell into an interception device is high,[265] their low cost and small size makes them an ideal choice for a technically sophisticated criminal.

3. Advances in Passive Interception

Just as the software-defined radio revolution and the availability of open source cellular radio software have lowered the cost of active interception, they have also enabled researchers and hobbyists to create low-cost, passive interception devices. Such capacity to receive the signals transmitted over the air between phones and cellular networks should not automatically enable interception of the contents of telephone calls. After all, modern cellular networks generally use encryption technologies to protect communications.[266] The wireless industry, however, continues to use insecure encryption algorithms, many of which were created behind closed doors, without review by independent cryptography experts.[267] Moreover, some developers of

264. Golde, Redon & Borgaonkar, *supra* note 263, at 7 ("This allows an attacker to impersonate any operator by utilizing a rogue femtocell as an inexpensive 3G IMSI-Catcher and wiretap device. Consequently, adversaries can intercept mobile communication by installing the device in the radio range of a victim."); Erica Fink & Laurie Segall, *Femtocell Hack Reveals Mobile Phones' Calls, Texts and Photos*, CNNMONEY (July 15, 2013), http://money.cnn.com/2013/07/15/technology/security/femtocell-phone-hack/index.html ("In a demonstration . . . researchers . . . covertly recorded one of our phone conversations and played it back for us. They were also able to record our browsing history, text messages, and even view pictures we sent from one smartphone to another by hacking the network extender.").

265. It is possible, and in fact, likely, that sophisticated users will in time automate much of the difficult work required to modify the software running on femtocells, thus lowering the technical barriers that currently prevent less-sophisticated users from using femtocells to intercept calls. *Cf*. *supra* note 256.

266. This is not always the case. *See supra* note 37 (describing countries where encryption is not used for voice communications). Moreover, even when voice communications are encrypted, text messages may not be. *See* Magnus Glendrange et al., Decoding GSM 141 (unpublished Masters thesis, Norwegian University of Science and Technology) (June 2010), *available at* http://www.diva-portal.org/smash/get/diva2:355716/FULLTEXT01.pdf ("When the authors of this thesis asked the various operators, [the Norwegian cellular carrier] Telenor was the only company to admit that they were *not* encrypted . . . . It seems to be optional for the operator to encrypt SMS, because we have reports of it being encrypted in Germany.").

267. *See* Orr Dunkelman, Nathan Keller & Adi Shamir, *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony*, IACR EPRINT ARCHIVE (2010), http://eprint.iacr.org/2010/013.pdf ("GSM cellular telephony is protected by the A5 family of cryptosystems. The first two members of this family, A5/1 . . . and A5/2 . . . were

these standards have alleged that they were weakened at the request of Western intelligence services.[268]

Predictably, cryptography researchers have repeatedly discovered critical security flaws in the encryption algorithms designed and deployed by the cellular industry.[269] Such flaws can be exploited to decipher the encrypted cellular signals captured with passive monitoring equipment. Moreover, even after researchers demonstrated that these encryption algorithms are vulnerable to interception, the cellular industry — including major U.S. wireless carriers — continues to use them,[270] perhaps because of the significant cost of upgrading to newer, more secure technology.[271]

---

designed in the late 1980s in an opaque process and were kept secret until they were reverse engineered in 1999 from actual handsets.").

268. *See* John Perry Barlow, *Decrypting the Puzzle Palace*, COMMC'NS OF THE ACM (July 1992), http://groups.csail.mit.edu/mac/classes/6.805/articles/digital-telephony/Barlow_decrypting_puzzle_palace.html (describing the adoption by the U.S. cellular industry of intentionally vulnerable encryption algorithms known to be "pitifully easy to break" as a result of pressure by the NSA); Arild Færaas, *Sources: We Were Pressured To Weaken the Mobile Security in the 80's*, AFTENPOSTEN (Jan. 9, 2014), http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html (interviewing several experts involved with the creation of the original GSM A5/1 standard who claim that it was intentionally weakened as a result of pressure from the British government); John Markoff, *Researchers Crack Code in Cell Phones*, N.Y. TIMES (Apr. 14, 1998), http://www.nytimes.com/1998/04/14/business/researchers-crack-code-in-cell-phones.html ("[A] digital key used by G.S.M. may have been intentionally weakened during the design process to permit Government agencies to eavesdrop on cellular telephone conversations."); Posting of Ross Anderson, rja14@cl.cam.ac.uk to UK.Telecom Google Group, https://groups.google.com/forum/#!forum/uk.telecom (June 17, 1994), https://groups.google.com/forum/#!msg/uk.telecom/TkdCaytoeU4/Mroy719hdroJ ("[T]here was a terrific row between the NATO signals agencies in the mid 1980's [sic] over whether GSM encryption should be strong or not. The Germans said it should be, as they shared a long border with the Evil Empire; but the other countries didn't feel this way.").

269. For example, the COMP128 cellular authentication algorithm was broken in two hours by Ian Goldberg and David Wagner, then graduate students at UC Berkeley. *See* Posting of Marc Briceno, marc@scard.org, to ukcrypto@maillist.ox.ac.uk (Oct. 21, 1999) [hereinafter Posting of Briceno], *available at* http://cryptome.org/jya/gsm-weak.htm (revealing that he reverse-engineered the COMP128 and A5/2 algorithms "during evenings and on weekends over the course of a few months on a budget of well below $100," and that Ian Goldberg and David Wagner then cryptanalyzed and promptly broke the algorithms in 2 hours for COMP128 and 2 days for A5/2); David Wagner, Ian Goldberg & Marc Briceno, *GSM Cloning*, ISSAC ARCHIVE (Apr. 13, 1998), http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html.

270. *See infra* note 281.

271. As Steve Babbage, the Chairman of ETSI SAGE observed in 2007, the cost to the wireless carriers of replacing old cellular network equipment with newer, more secure technology is likely a major reason for the carriers' decade long delay in replacing algorithms known to be significantly flawed. *See* Steve Babbage, *An Update from ETSI SAGE*, SECURITY ALGORITHMS GROUP OF EXPERTS 3 n.3 (2007), *available at* http://www.etsi.org/images/files/securityworkshop2007/Security2007S7_4_Steve_Babbage.pdf ("GSM encryption is performed in the base station — and there are an awful lot of base stations in an operator network. Introducing substantially different algorithms typically requires a hardware upgrade, not just a software change. So upgrading a network to support a new GSM algorithm is very expensive.").

One of the most widely used cellular telephone encryption algorithms, A5/1, was created by the wireless industry in 1988.[272] A weakened version intended for use by non-Western countries, known as A5/2, was developed five years later.[273] The industry did not publish these algorithms, but in 1999 they were reverse engineered and finally subjected to review by independent security experts.[274] A team of graduate students broke the weakened,[275] "export-grade" A5/2 algorithm in only a few hours after it was published.[276] Several months later, a team of cryptographers discovered a critical flaw in the stronger A5/1 algorithm, opening the door to practical, real-time decryption of A5/1 protected communications.[277]

Even though the cryptography community considered A5/2 broken in 1999, the cellular industry did not phase out its use until 2007,[278] and then only because new research demonstrated that the

---

272. *See* SECURITY ALGORITHMS GROUP OF EXPERTS (SAGE), REPORT ON THE SPECIFICATION AND EVALUATION OF THE GSM CIPHER ALGORITHM A5/2, ETSI TECHNICAL REPORT 278 (Mar. 1996), *available at* http://www.etsi.org/deliver/etsi_etr/200_299/278/01_60/etr_278e01p.pdf.

273. *See id*. ("SAGE started work on A5/2 in November 1992 and delivered the final specification and test data to the MoU Security Rapporteur on the 31 March 1993.").

274. *See* Dunkelman, Keller & Shamir, *supra* note 267.

275. The design goal of A5/2 was to "protect traffic on the GSM radio path so that such traffic is no more vulnerable to eavesdropping than on a Public Switched Telephone Network (PSTN) telephone line . . . ." The algorithm apparently passed this low bar, and "all members of SAGE stated [prior to the algorithm's release] that they were satisfied that the algorithm was suitable to protect against eavesdropping on the GSM radio path . . . ." *See* SECURITY ALGORITHMS GROUP OF EXPERTS (SAGE), *supra* note 272, at 9, 11. However, by 2007, after academic researchers had demonstrated significant security flaws in the algorithm, even the Chairman of the SAGE group acknowledged that the "A5/2 encryption algorithm for GSM is extremely weak — it provides no protection at all against eavesdropping." *See* Babbage, *supra* note 271, at 2.

276. *See* Posting of Briceno, *supra* note 269; E-mail from David Wagner to author (Mar. 17, 2014, 01:04 AM EDT) ("It took us about 5 hours to devise a break of A5/2.") (on file with author); Ian Goldberg et al., *The (Real-Time) Cryptanalysis of A5/2*, CRYPTO '99 (Aug. 26, 1999), *available at* http://www.cs.berkeley.edu/~daw/tmp/a52-slides.ps.

277. *See* Alex Biryukov et al., *Real Time Cryptanalysis of A5/1 on a PC*, FAST SOFTWARE ENCRYPTION WORKSHOP (2000), *available at* http://cryptome.org/a51-bsw.htm (updating a paper published in LECTURE NOTES IN COMPUTER SCIENCE 1978, at 1–18 (1999)). During the decade that followed the A5/1 research by Biryukov and Shamir, several other research teams improved on this work, to make it more efficient to break. *See, e.g*., Eli Biham & Orr Dunkelman, *Cryptanalysis of the A5/1 GSM Stream Cipher*, *in* PROGRESS IN CRYPTOLOGY, PROCEEDINGS OF INDOCRYPT '00, LECTURE NOTES IN COMPUTER SCIENCE 1977 43 (2000); Alexander Maximov et al., *An Improved Correlation Attack on A5/1*, *in* PROCEEDINGS OF THE 11TH INTERNATIONAL CONFERENCE ON SELECTED AREAS IN CRYPTOGRAPHY (SAC'04), LECTURE NOTES IN COMPUTER SCIENCE 3357 1 (2005); Karsten Nohl, *Attacking Phone Privacy*, SECURITY RESEARCH LABS, at 6 (July 28, 2010), https://srlabs.de/blog/wp-content/uploads/2010/07/Attacking.Phone_.Privacy_Karsten.Nohl_1.pdf.

278. *See Withdrawal of A5/2 Algorithm* [sic] *Support*, OSMOCOM SECURITY, http://security.osmocom.org/trac/wiki/A52_Withdrawal (Nov. 12, 2010). *See generally* Harald Welte, *A Brief History on the Withdrawal of the A5/2 Ciphering Algorithm in GSM*, HARALD WELTE'S BLOG (last modified Nov. 12, 2010), www.advogato.org/person/LaForge/diary.html?start=137.

methods used to attack A5/2 could be used to attack the security of Western A5/1 networks as well.[279] Today, the A5/1 algorithm, created in 1988 and thoroughly broken a decade ago, remains the most widely deployed cellular encryption algorithm in the world.[280] Indeed, wireless carriers AT&T and T-Mobile still use the A5/1 algorithm for their older "2G" networks in the United States.[281]

Information about the strength of the encryption algorithms chosen by carriers, or whether encryption is used at all, is not readily made available to consumers, who reasonably might be alarmed to learn that the wireless carriers are not using the most secure encryption available (or in some cases, any at all) to protect their communications. Indeed, the GSM standard requires that phones be capable of displaying a warning when no encryption is in use.[282] However, the standard also permits wireless carriers to disable the encryption indicator, something that most do.[283] Likely due to the fact that it was generally disabled and thus not displayed to consumers, many phone manufacturers, including some of the largest phone manufacturers such as Apple, Samsung, and Huawei, do not support the encryption warning feature in their phones.[284] As such, there is generally no easy way for consumers to determine when their calls are unencrypted or only protected with weak encryption algorithms.

Although the academic research community has long documented the flaws in the encryption algorithms used by wireless carriers, these

---

279. The primary motivation for the cellular industry to withdraw A5/2 was not concern for the privacy of users in countries where the weak A5/2 algorithm was used, but rather, because the availability of A5/2 support in handsets threatened the security of phone calls in countries where the more-secure A5/1 algorithm was used. *See* Welte, *supra* note 278 ("Since they [sic] key generation for A5/1 and A5/2 is the same, a semi-active downgrade attack can be used to retroactively break previously-recorded, encrypted A5/1 calls. The only solution to this problem is to remove A5/2 from all equipment, to make sure the downgrade is not possible anymore.").

280. *See* Timberg & Soltani, *supra* note 8 ("More than 80 percent of cellphones worldwide use weak or no encryption for at least some of their calls . . . .").

281. *See GSM Security Country Report: USA*, SECURITY RESEARCH LABS, at 4 (Aug. 2013), *available at* http://gsmmap.org/assets/pdfs/gsmmap.org-country_report-United_States_of_America-2013-08.pdf; E-mail from Karsten Nohl to author (Apr. 6, 2014, 11:19 PM PDT) (on file with author) (describing the continued use of A5/1 "by AT[&]T and T-Mobile, but only for 2G voice and SMS" while 3G "uses a much improved cipher, that currently nobody knows how to crack" and A5/0 is used in the United States "only for less important transaction[s] such as regular [network] updates, but not for calls or SMS").

282. *See* Iosif Androulidakis et al., *Ciphering Indicator Approaches and User Awareness*, 2012 MAEJO INT'L J. SCI. & TECH. 514, 516, *available at* http://www.mijst.mju.ac.th/vol6/514-527.pdf.

283. *See* DEFCONConference, *supra* note 255, at 07:10 ("So, every sim card that I have ever seen in my entire life, and I've seen a few, from various networks around the world, every single one of them has [the warning disabled], every single operator that I've ever seen disables that warning message.").

284. Androulidakis et al., *supra* note 282, at 519 ("Nine different manufacturers in the considered dataset (Sharp, Samsung, Qtek, HTC, Motorola, LG, Huawei, Chinabuye and Apple) did not employ a Ciphering Indicator, although this is required by the standards . . . .").

vulnerabilities could only be exploited by those with the resources to buy or build interception and decryption equipment. But just as software-defined radio technology has lowered the cost of active interception, so too has it provided researchers and hobbyists with the means to receive cellular signals that can then be deciphered using open source software that implements decade-old academic cryptographic research.[285] Passive interception technology that once cost tens of thousands of dollars can now be built at home for as little as $15.[286] Similarly, whereas cellular interception was once a black art practiced by those in the intelligence community, today, professors assign the task of decrypting cellular communications to their computer science students.[287]

The widespread availability of low-cost radio hardware, fast personal computers, and free open source cellular interception and cryptanalysis software has made passive interception possible for any interested tech-savvy person, including criminals, enabling them to access conversations and other data previously only available to governments.[288] These security threats are discussed next.

---

285. *See* Glendrange et al., *supra* note 266, at 2 (stating that, due to its expense and complexity "[a]nalyzing and capturing GSM traffic was up until recently an unexplored area" but anticipating that soon "anyone with [an] interest in GSM security [will be enabled] to investigate the theoretical security principles through practical approach"); *A5/1 Decryption*, SECURITY RESEARCH LABS, https://opensource.srlabs.de/projects/a51-decrypt (last visited Dec. 18, 2014) (the website for the Kraken tool, which "allows the 'cracking' of A5/1 keys used to secure GSM 2G calls and SMS.").

286. *See* Jon Borland, *$15 Phone, 3 Minutes All That's Needed To Eavesdrop on GSM Call*, ARS TECHNICA (Dec. 29, 2010), http://arstechnica.com/gadgets/2010/12/15-phone-3-minutes-all-thats-needed-to-eavesdrop-on-gsm-call/; Posting of Lucky Green, [email unavailable], to cryptography@c2.net (Dec. 5, 1999), http://www.mail-archive.com/cryptography@c2.net/msg02532.html ("I know how to build a GSM interception station using off-the-shelf hardware and [an Intel Pentium II processor] running Linux for a total cost of well below USD 10k.").

287. *See* Gerhard Schneider, Konrad Meier & Dennis Wehrle, *Practical Exercise on the GSM Encryption A5/1* (Feb. 23, 2011), https://web.archive.org/web/20131228091106/http://www.data.ks.uni-freiburg.de/download/misc/practical_exercise_a51.pdf (accessed through the Internet Archive Index).

288. It should be noted that the research team that has in recent years lead the way in demonstrating significant, practical flaws in the A5/1 algorithm has intentionally not published step-by-step instructions to decrypt calls. *See* Posting of Karsten Nohl, nohl@virginia.edu, to A51@lists.srlabs.de (Aug. 11, 2013), https://lists.srlabs.de/pipermail/a51/2013-August/001268.html ("We are not publishing attack tutorials. The line we are walking — between warning about possible abuse and enabling it — is already very fine."). However, it is almost certain that others will fill this void by documenting the process.

VI. OUR VULNERABLE CELLULAR NETWORKS CAN BE AND ARE EXPLOITED BY OTHERS

The U.S. and other select global powers no longer enjoy a domestic monopoly over the use of cellular interception technology.[289] Accordingly, a much larger number of hostile foreign intelligence serservices can and, almost certainly, are using the technology in this country for espionage. Similarly, if cellular interception technology is not already in use by criminals, the paparazzi, and tech-savvy creepy neighbors, it is only a matter of time before they acquire and use it too. This Part discusses these current and possible future threats.

A. Foreign Governments

Cellular interception technology can be a critical tool in intelligence operations.[290] In contrast to law enforcement surveillance, for example, where the assistance of a wireless carrier is often available, intelligence agencies operating without the knowledge or assistance of local governments cannot obtain information from wireless carriers.[291] As such, cellular interception devices are often the only way for intelligence agencies to monitor the communications of targets.

Indeed, as a result of the disclosures to the media by Edward Snowden, it is now clear (and not surprising) that the U.S. National Security Agency ("NSA") uses both active and passive cellular interception technology. The NSA's Special Collection Service reportedly uses passive cellular interception devices installed at U.S. embassies and consulates around the world to spy on the telephone calls of foreign leaders.[292] More specifically, an internal NSA surveillance product catalog describes active cellular interception devices that are available for use by agents conducting intelligence operations.[293]

Just as U.S. intelligence agencies use cellular interception technology to perform surveillance in foreign countries, so too do foreign

289. *See supra* Part V.

290. *See* Morrison Affidavit 2012, *supra* note 50; *supra* Part II.B.

291. *See supra* Part II.B.

292. *See DRTBOX and the DRT Surveillance Systems*, TOP LEVEL TELECOMM'S (Nov. 27, 2013), http://electrospaces.blogspot.com/2013/11/drtbox-and-drt-surveillance-systems.html (describing the DRT family of cellular surveillance products manufactured by Boeing and analyzing their likely use by the NSA, based on references to "DRTBox" in NSA documents leaked by Edward Snowden); *supra* note 90.

293. *See CANDYGRAM — GSM Telephone Tripwire*, http://leaksource.files.wordpress.com/2013/12/nsa-ant-candygram.jpg (last visited Dec. 18, 2014) ("Mimics GSM cell tower of a target network . . . . Typical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets."); Jacob Appelbaum, Judith Horchert & Christian Stöcker, *Shopping for Spy Gear: Catalog Advertises NSA Toolbox*, SPIEGEL ONLINE (Dec. 29, 2013), http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

intelligence agencies operating in Washington D.C.[294] In a 2012 book, national security reporters Marc Ambinder and D.B. Grady hinted at the existence of cellular surveillance activities by foreign governments, revealing that "[t]he FBI has quietly removed from several Washington, D.C.-area cell phone towers, transmitters that fed all data to . . . foreign embassies."[295] When asked about the claim by the Washington Post, the FBI declined to comment.[296] However, a former FBI deputy director told Newsweek in the summer of 2014 that "[t]his type of technology has been used in the past by foreign intelligence agencies here and abroad to target Americans, both [in the] U.S. government and corporations . . . . There's no doubt in my mind that they're using it."[297]

As President Obama has noted, "We know that the intelligence services of other countries . . . are constantly probing our government and private sector networks and accelerating programs to listen to our conversations . . . . " [298] It is for that reason, he added, that "BlackBerrys and iPhones are not allowed in the White House Situation Room."[299] The importance of those security rules was proven after a team of technical experts revealed in the fall of 2014 that they had detected, with sophisticated anti-surveillance equipment, tell-tale signs of IMSI catchers in eighteen locations in the Washington D.C. area, including near the White House, Congress, and several foreign embassies.[300]

Although the NSA takes steps to protect the communications of the President and other senior national security officials from foreign

---

294. *See* Matthew M. Aid, *The Spies Next Door*, FOREIGN POL'Y (Sept. 21, 2012), http://www.foreignpolicy.com/articles/2012/09/21/the_spies_next_door ("Almost half of the 200,000 men and women who belong to the U.S. intelligence community work in Washington, *as do several thousand foreign intelligence officers who operate openly from dozens of embassies and international organizations in the U.S. capital, trawling the landscape for secrets*.") (emphasis added).

295. *See* MARC AMBINDER & D.B. GRADY, DEEP STATE: INSIDE THE GOVERNMENT SECRECY INDUSTRY 245 (2013).

296. Timberg & Soltani, *supra* note 8.

297. Jeff Stein, *New Eavesdropping Equipment Sucks All Data off Your Phone*, NEWSWEEK (June 22, 2014), http://www.newsweek.com/2014/07/04/your-phone-just-got-sucked-255790.html.

298. *See* Barack Obama, President of the United States, Speech on NSA Reforms (Jan. 17, 2014), *in Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, WASH. POST (Jan. 17, 2014), http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

299. *Id*.

300. *See* Ashkan Soltani & Craig Timberg, *Tech Firm Tries To Pull back Curtain on Surveillance Efforts in Washington*, WASH. POST (Sept. 17, 2014), http://www.washingtonpost.com/world/national-security/researchers-try-to-pull-back-curtain-on-surveillance-efforts-in-washington/2014/09/17/f8c1f590-3e81-11e4-b03f-de718edeb92f_story.html.

intelligence agencies, they are the exception, not the norm.[301] It is likely that many Members of Congress and their staff do not receive special assistance or protection from surveillance in the United States.[302] Similarly, there are many other people who participate, directly or indirectly, in this country's policy process — including journalists, lawyers, lobbyists, researchers, and activists — whose communications are intelligence-rich, vulnerable, and likely targeted by foreign intelligence agencies.

Moreover, cellular interception equipment is equally useful for non-political espionage conducted by foreign governments. Specifically, this technology can be used in business centers like New York or Silicon Valley for industrial espionage or to gain insider knowledge by monitoring the communications of business executives, financiers, and entrepreneurs.[303]

B. Non-Government Use of Cellular Surveillance Technology

If cellular interception technology were still prohibitively expensive and exclusively available to governments engaged in foreign and domestic surveillance, the communications of the average law-abiding American would rarely be targeted.[304] After all, intercepting telephone calls on U.S. soil will presumably focus their efforts on the tiny percentage of Americans whose communications have some significant strategic or intelligence value.

---

301. *See* Michael S. Schmidt & Eric Schmitt, *Obama's Portable Zone of Secrecy (Some Assembly Required)*, N.Y. TIMES, Nov. 10, 2013, at A1, *available at* http://www.nytimes.com/2013/11/10/us/politics/obamas-portable-zone-of-secrecy-some-assembly-required.html ("Countermeasures are taken on American soil as well. When cabinet secretaries and top national security officials take up their new jobs, the government retrofits their homes with special secure rooms for top-secret conversations and computer use.").

302. *See* Letter from Tom Wheeler, Chairman, FCC, to Rep. Alan M. Grayson (Aug. 1, 2014), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2014/db0822/DOC-328995A1.pdf (responding to inquiry by Rep. Grayson as to how Congress can protect their cellular communications from interception by encouraging Rep. Grayson and his colleagues in Congress to "utilize resources the Commission has made available to educate and inform regarding communications goods and services," including "several consumer publications aimed at increasing consumer awareness of [interception] risks").

303. *See* James Clark, *French Spies Listen in to British Calls*, SUNDAY TIMES (U.K.), Jan. 23, 2000, *available at* Factiva, Doc. No. st00000020010817dw1n000of ("French intelligence is intercepting British businessmen's calls . . . . Eavesdroppers can 'pluck' GSM digital mobile phone signals from the air by targeting individual numbers or sweeping sets of numbers. Targets have included executives at British Aerospace, British Petroleum and British Airways . . . .").

304. The strategic targeting practices of foreign governments do not, however, completely insulate innocent, law-abiding Americans from having their communications monitored incidentally by the United States and foreign government agencies. As described in Part II, this surveillance technology is by its very nature overbroad in its operation, capturing data about many other phones in the vicinity of the area where it is used.

With respect to the average American's exposure to private communications interception, however, history appears to be repeating itself. Just as the radio scanners of the 1990s enabled nearly anyone to intercept a neighbor's analog phone communications, modern cellular interception devices are now available for purchase over the Internet from surveillance technology resellers around the world for a few thousand dollars each.[305] Moreover, they are far easier to use than the homemade models built by researchers,[306] making them an attractive tool for criminals, private investigators, and paparazzi.[307]

In the Czech Republic, for example, law enforcement and intelligence officials have voiced concerns about the threat posed by cellular interception technology. In 2012, the head of the Czech Criminal Police unit for wiretapping told the national public radio service that his team had detected non-police active interception devices in use around the country.[308] Similarly, the ex-head of the Czech Military Intelligence Agency expressed fears about potential widespread availability and sale of such technology, stating that "if their use will not be in any way regulated, and access to these devices will not be in any way controlled, then a regular citizen can do absolutely nothing [to safeguard their communications]."[309] He speculated that the most likely private users of the devices were security firms and rival businesses engaged in industrial espionage.[310]

In China, cellular interception devices are perhaps more widely available than in any other country in the world. In the spring of 2014, Chinese police shut down twenty-four different factories manufacturing illegal IMSI catchers.[311] These devices are in widespread use by criminal gangs, apparently not for surveillance or espionage, but rather, to send spam and fraudulent text messages that lure unwitting victims to phishing sites.[312] Specifically, using these devices, fraudsters send tens of millions of messages per day to unsuspecting consumers with spoofed origin phone numbers normally used by online

---

305. *See supra* Part V.

306. *See supra* Part V.B.1.

307. We are not suggesting that it would be legal for private parties to intercept the conversations of others. The chance of being discovered intercepting calls, however, is extremely low, even more so when passive surveillance technology is used.

308. *See* Masha Volynsky, *Spy Games Turn Real as Eavesdropping Technology Spreads*, RADIO PRAGUE (Aug. 16, 2012), http://www.radio.cz/en/section/curraffrs/spy-games-turn-real-as-eavesdropping-technology-spreads.

309. *Id*.

310. *Id*.

311. *See Chinese Police Bust Major Telecom Fraud Ring*, XINHUA, *available at* http://www.chinadaily.com.cn/china/2014-04/29/content_17474783.htm (last updated Apr. 29, 2014).

312. *See* Russel Brandom, *Phony Cell Towers Are the Next Big Security Risk*, VERGE (Sept. 18, 2014), http://www.theverge.com/2014/9/18/6394391/phony-cell-towers-are-the-next-big-security-risk.

banks and other trusted parties.[313] According to one Chinese mobile security expert, "It's very lucrative to have a [fake] tower device right now. People will pay big money for it . . . ."[314]

While commercial cellular interception technology is, for now, probably too expensive for the average stalker or garden variety criminal, the cost of these devices will, like all technology, decrease over time.[315] At just a few thousand dollars each, however, commercial cellular interception devices are already affordable for sophisticated domestic or multi-national criminal organizations, companies engaging in industrial espionage, private investigators, and paparazzi. And for the technically skilled criminal, no matter the scale of his operations, cellular surveillance technology is already affordable.[316]

Although cellular surveillance devices are not *yet* in widespread private use in the United States,[317] they are certainly no longer a secret. To suggest otherwise is to embrace and propagate a fiction; these technologies have been globalized and democratized, and the vulnerabilities they exploit now threaten the privacy of hundreds of millions of Americans who use cellular telephones to communicate. Indeed, the use of cellular interception devices in India and the Czech Republic paints a worrisome picture of the potential threat. Even so, U.S. government agencies continue to treat cellular surveillance equipment as a closely guarded secret, even protecting the name of the equipment they use.[318] As discussed next, the consequence of embracing this erroneous, tendentious narrative, which grants surveillance priority over the security of communication networks, is that the American public remains vulnerable to cellular surveillance by a variety of non-U.S. government actors.

VII. A HIGH PRICE TO PAY FOR THE FICTION OF SECRECY

The analog-phone vulnerabilities of the 1990s were no secret. The technology required to intercept calls was widely available and several high-profile abuses led to front-page scandals involving the com-

313. *Id*.

314. *Id*.

315. *See generally* Douglas McCormick, *Wright's Law Edges out Moore's Law in Predicting Technology Development*, IEEE SPECTRUM (July 25, 2012), http://spectrum.ieee.org/tech-talk/at-work/test-and-measurement/wrights-law-edges-out-moores-law-in-predicting-technology-development (describing a research paper that compares various models, including Moore's Law, all of which attempt to predict the decrease in the price of technologies over time).

316. *See supra* Part V.B.1.

317. This does not mean they have not been used at all. According to national security journalist Marc Ambinder, "The Secret Service has caught people using Sting[R]ays to collect personal data for use in financial fraud cases." *See* E-mail from Marc Ambinder to author (May 13, 2013, 11:30 PM PDT) (on file with author).

318. *See supra* Part IV.

munications of the rich and powerful. In response, Congress held hearings, the cellular industry weighed in, and, ultimately, the FCC promulgated regulations intended to limit the ease with which interception technology could be obtained.[319] Although the approach adopted by policy makers and regulators — seeking to prohibit the sale of interception equipment, rather than mandating technical solutions capable of securing communications from interception — was ineffective, Congress and the FCC at least acknowledged the problem and did *something* to try to address it.

The Congress of the 1990s held public hearings focused on cellular interception vulnerabilities;[320] the Congress of the 2010s has not. The FCC of the 1990s adopted regulations intended to protect cellular communications from interception;[321] the FCC of the 2010s perpetuates the fiction that cellular interception is a secret capability available only to government agencies by shielding information about cellular interception equipment from public disclosure.[322] Whereas the cellular vulnerabilities of the 1990s were treated as a threat to the nation's cellular network, today, DHS, whose stated mission includes protecting critical infrastructure and information networks,[323] also appears to have embraced the sensitive source and method narrative.[324]

In 2013, acting FCC Chairwoman Mignon Clyburn stated, "Protecting consumer privacy is a key component of [the FCC's] mission to serve the public interest."[325] Her predecessor, former FCC Chairman Julius Genachowski, similarly acknowledged that Congress had directed the Commission to "protect the privacy of consumers who rely on our Nation's communications infrastructure."[326] Over the past two decades, however, the FCC appears to have done little other than accommodate and perpetuate the fictional secrecy narrative authored

---

319. *See supra* Part I.

320. *Id*.

321. *Id*.

322. *See* Letter from Julius P. Knapp, Chief, Office of Eng'g & Tech., FCC, to author (Feb. 29, 2012), *available at* http://files.cloudprivacy.net/FOIA/FCC/fcc-stingray-reply.pdf ("[W]e are withholding certain intra-agency and interagency e-mails and documents because they are classified or because taken together with other information they could endanger national and homeland security.").

323. *Mission*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/mission (last modified Aug. 8, 2012) ("[DHS] works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems.").

324. *See supra* Part III.

325. Statement of Mignon Clyburn, Acting Chairwoman, FCC, Re: Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, CC Docket No. 96-115 (June 27, 2013), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0627/FCC-13-89A2.pdf.

326. *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci. and Transp.*, 111th Cong. 3 (2010) (statement of Julius Genachowski, Chairman, FCC), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-111shrg67686/html/CHRG-111shrg67686.htm.

by law enforcement agencies and cellular surveillance equipment manufacturers.[327] Indeed, the agency continues to grant equipment authorizations (and requested protections from public disclosure) for each new cellular surveillance product the Harris Corporation seeks to market to law enforcement agencies.[328]

Together with the FCC, DHS shares the responsibility of protecting the security of America's civilian telephone networks. DHS is also a law enforcement agency, with component agencies that have spent millions of dollars on StingRays and other cellular interception equipment.[329] Moreover, DHS funds the acquisition of cellular surveillance equipment by state and local law enforcement agencies.[330] Likewise, as the primary regulator of the wireless and wireline carriers, the FCC has repeatedly used its regulatory powers to force telecommunications companies to facilitate surveillance by law enforcement and intelligence agencies.[331] These two agencies thus

---

327. *See supra* Part IV.B.

328. *See supra* note 191.

329. *See* Kelly, *supra* note 21.

330. *See* STAFF OF PERMANENT SUBCOMM. ON INVESTIGATIONS OF THE S. COMM. ON HOMELAND SEC. AND GOVERNMENT AFFAIRS, 112TH CONG., REP. ON FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS 81 (Oct. 3, 2012), *available at* http://www.hsgac.senate.gov/download/?id=49139e81-1dd7-4788-a3bb-d6e7d97dde04 (describing the use of a FEMA grant to purchase "sophisticated cell phone tracking devices" by the Washington D.C. Homeland Security and Emergency Management Agency); CITY OF TACOMA, WA, CITY COUNCIL MINUTES (Mar. 19, 2013), *available at* http://cms.cityoftacoma.org/cityclerk/Files/CityCouncil/Minutes/2013/CCMin20130319.pdf ("Authorizing the execution of a grant agreement with the U.S. Department of Homeland Security Port Security Grant Program in the amount of $188,814.31 . . . [to purchase from the] Harris Corporation . . . technical support equipment to assist in the prevention, detection, response, and recovery of improvised explosive devices."); Michael Bott & Thom Jensen, *Cellphone Spying Technology Being Used Throughout Northern California*, NEWS 10 (Mar. 6, 2014), http://www.news10.net/story/news/investigations/watchdog/2014/03/06/cellphone-spying-technology-used-throughout-northern-california/6144949/ ("StingRays are being paid for mostly by Homeland Security grant money distributed by the California Emergency Management Agency, under programs such as the Urban Areas Security Initiative (UASI) or the State Homeland Security Program (SHSP).").

331. The FCC has repeatedly used the license granting process to extract surveillance enabling concessions from service providers that are not required by law. *Fourth Amendment and the Internet: Hearing Before the Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 106th Cong. 135 (2000) (statement of Stewart Baker, Partner, Steptoe & Johnson LLP), *available at* http://commdocs.house.gov/committees/judiciary/hju66503.000/hju66503_0f.htm (noting that "[t]he FBI and the Justice Department have intervened repeatedly at the FCC to try to deny licenses to companies that have not been fully cooperative" and citing specific examples of such practice); Craig Timberg & Ellen Nakashima, *Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance*, WASH. POST (July 6, 2013), http://www.washingtonpost.com/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html ("In deals involving a foreign company, say people familiar with the process, the FCC has held up approval for many months while the squadron of lawyers dubbed Team Telecom developed security agreements that went beyond what's required by the laws governing electronic eavesdropping."). Responding to a specific request by the DOJ, the FCC has also required telephone companies to retain telephone call records. Douglas Cox, *More Misleading Information from ODNI on NSA Telephone Metadata Collection*, DOCUMENT EXPLOITATION (July 24, 2013), http://www.docexblog.com/2013/07/more-

attempt to satisfy two, sometimes competing, jurisdictional mandates:[332] enabling or engaging in surveillance on the one hand, while seeking to ensure the security of communications networks, on the other. These dual roles and objectives come into conflict, in theory and practice, when choices must be made to privilege either surveillance or security.

With respect to the dual surveillance and security responsibilities under the jurisdiction of these federal agencies, an uncritical adoption of the law enforcement narrative can suppress an equally compelling counter-narrative: Americans' cellular communications are vulnerable to interception by foreign governments and criminals. We don't know if or to what extent officials at the FCC or DHS have made an actual policy choice to privilege cellular interception over the security of cellular networks. Are officials, by withholding information about cellular interception technology, uncritically perpetuating the sensitive source and method narrative or, much worse, are they participating in a strategic choice to embrace this fiction?

By viewing cellular interception equipment completely from a law enforcement agency perspective, policymakers and regulators are unlikely to address the underlying vulnerabilities in American cellular networks. To date, the government has made little effort publicly to address the cellular network vulnerabilities or to warn users about them. Meanwhile, the FCC and DHS have actively enabled the ongoing exploitation of these vulnerabilities by U.S. government agencies.

In response to a letter from Congressman Alan Grayson that cited an early online draft of this Article,[333] FCC Chairman Tom Wheeler announced that the Commission has formed a task force to investigate "illicit uses" of cellular surveillance technology. [334] Congressman Grayson's letter and Chairman Wheeler's announcement are the first direct, public statements by current U.S. government officials acknowledging the privacy and national security threats posed by cellular interception technology.

---

misleading-information-from-odni.html (noting that, in addition to implementing the policy requested by the DOJ, the FCC also "extended the legal retention period for as long as the DOJ said was necessary").

332. These are not the only agencies that have conflicting missions. The NSA has been criticized for prioritizing its offensive mission over defense. Bruce Schneier, *It's Time to Break up the NSA*, CNN OPINION (Feb. 20, 2014), http://www.cnn.com/2014/02/20/opinion/schneier-nsa-too-big/index.html ("[The NSA] is an agency that prioritizes intelligence gathering over security, and that's increasingly putting us all at risk.").

333. Letter from Alan M. Grayson to Tom Wheeler, *supra* note 29 (citing a draft of this Article as well as a Newsweek article that describes a demonstration of IMSI catchers for congressional staff organized by one of this Article's authors).

334. Letter from Tom Wheeler to Alan M. Grayson, *supra* note 302 ("I have recently established a task force to initiate immediate steps to combat the illicit and unauthorized use of IMSI catchers. The mission of this task force is to develop concrete solutions to protect the cellular network systemically from similar unlawful intrusions and interceptions.").

While the FCC's task force is perhaps a positive first step, to the extent that it focuses only on the illicit uses of the surveillance technology without addressing the underlying network vulnerabilities exploited by IMSI catchers, it will do little to address the real cybersecurity threat.[335] To address these network vulnerabilities, however, because all parties' surveillance technology exploit the same network vulnerabilities, policymakers will have to grapple with the tension inherent in facilitating "lawful" IMSI catcher use by law enforcement and prohibiting unlawful use by a host of bad actors. That is, there is no way to allow law enforcement to use cellular surveillance devices without also leaving networks vulnerable to criminals and foreign governments.

If the existence and knowledge of these vulnerabilities were truly a secret, and the technology that exploits them were only available to U.S. government agencies, privileging law enforcement equities might be a reasonable policy choice. Such a choice would only be warranted, however, if law enforcement surveillance capabilities could be protected without placing the American public at risk. But as this Article has illustrated, this scenario does not describe reality.

IMSI catcher secrecy is a fairytale, while the long-term impact of the technology may lead to a privacy and security nightmare. Indeed, many of the security flaws exploited by cellular surveillance devices were publicly documented by academic security researchers a decade ago.[336] In the years since, numerous foreign governments have acquired surveillance devices that exploit those same vulnerabilities.[337] Moreover, they are readily available to technologically sophisticated criminals, private investigators, and the paparazzi. Meanwhile, law-abiding citizens and businesses remain in a government-willed darkness on the matter, exposed to a myriad of interception risks.

If policymakers understood cellular network vulnerabilities and treated them as part of the existing debate about cybersecurity, informed public discourse about the balance of risks and rights could begin. The cybersecurity debate and the rightful place of cellular network security in that discourse are addressed next.

VIII. FOCUSING ON CYBERSECURITY

The United States faces a serious cybersecurity threat.[338] Foreign governments, such as China, have repeatedly hacked into the comput-

335. *See* Stephanie Pell, *We Must Secure America's Cell Networks — From Criminals and Cops*, WIRED (Aug. 27, 2014), http://www.wired.com/2014/08/we-must-secure-americas-cell-networks-from-criminals-and-cops-alike/; *infra* Part VIII.

336. *See supra* Part V.B.

337. *See supra* Part V.A.

338. Mitchell S. Kominsky, *The Current Landscape of Cybersecurity Policy: Legislative Issues in the 113th Congress*, HARVARD NAT'L SEC. J. (Feb. 6, 2014), http://harvardnsj.org/

er systems of government agencies and major U.S. companies, including technology firms and defense contractors, to steal intellectual property and classified information.[339] James Clapper, the Director of National Intelligence, and James Comey, the Director of the FBI, have both told Congress that cyber attacks are the most serious national security threat faced by the United States.[340]

In response to these cybersecurity threats and the warnings of senior government and industry officials, Congress has held numerous hearings and proposed legislation.[341] The White House has appointed a cybersecurity "czar,"[342] agencies' cybersecurity practices are regularly evaluated as part of the oversight process (often revealing serious problems),[343] and the government spends billions of dollar every year on cybersecurity.[344]

2014/02/the-current-landscape-of-cybersecurity-policy-legislative-issues-in-the-113th-congress/ ("Cybersecurity represents one of the most serious national security threats and economic challenges confronting our country. Cybercrime costs the United States approximately $100 billion annually . . . . [T]he cyber threat is quickly becoming the top priority for our national defense apparatus and private enterprise.").

339. *E.g.*, Jim Finkle, *Hacker Group in China Linked to Big Cyber Attacks: Symantec*, REUTERS (Sept. 17, 2013), http://www.reuters.com/article/2013/09/17/us-cyberattacks-china-idUSBRE98G0M720130917; Ellen Nakashima, *Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies*, WASH. POST (May 27, 2013), http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html; Michael Riley & Ben Elgin, *China's Cyberspies Outwit Model for Bond's Q*, BLOOMBERG (May 2, 2013), http://www.bloomberg.com/news/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets.html.

340. Greg Miller, *FBI Director Warns of Cyberattacks; Other Security Chiefs Say Terrorism Threat Has Altered*, WASH. POST (Nov. 14, 2013), http://www.washingtonpost.com/world/national-security/fbi-director-warns-of-cyberattacks-other-security-chiefs-say-terrorism-threat-has-altered/2013/11/14/24f1b27a-4d53-11e3-9890-a1e0997fb0c0_story.html ("FBI Director James B. Comey testified Thursday that the risk of cyberattacks is likely to exceed the danger posed by al-Qaeda and other terrorist networks as the top national security threat to the United States and will become the dominant focus of law enforcement and intelligence services."); *see also* Jim Garamone, *Clapper Places Cyber at Top of Transnational Threat List*, U.S. DEP'T OF DEF. (Mar. 12, 2013), http://www.defense.gov/news/newsarticle.aspx?id=119500.

341. *See, e.g.*, Cyber Intelligence Sharing and Protection Act, H.R. 3523, 112th Cong. (2012).

342. Michael Hardy, *New White House Cyber Czar Brings Intell Chops*, FED. COMPUTER WEEK (June 4, 2012), http://fcw.com/articles/2012/06/15/buzz-howard-schmidt-michael-daniel-cyber-czar.aspx.

343. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-137, INFORMATION SECURITY: WEAKNESSES CONTINUE AMID NEW FEDERAL EFFORTS TO IMPLEMENT REQUIREMENTS (2011), *available at* http://www.gao.gov/new.items/d12137.pdf; MINORITY STAFF OF THE HOMELAND SEC. & GOVERNMENTAL AFFAIRS COMM., THE FEDERAL GOVERNMENT'S TRACK RECORD ON CYBERSECURITY AND CRITICAL INFRASTRUCTURE (Feb. 4, 2014), *available at* http://www.hsgac.senate.gov/download/?id=8BC15BCD-4B90-4691-BDBA-C1F0584CA66A.

344. *See* Amber Corrin, *Budget Shows How Cyber Programs Are Spreading*, FED. COMPUTER WEEK (Apr. 12, 2013), http://fcw.com/Articles/2013/04/12/budget-cybersecurity.aspx ("The DHS figure includes nearly $500 million for cybersecurity research and development and almost $1 billion expressly for the protection of federal computers and networks against malicious cyber activity."); Andy Sullivan,

Although most of the cybersecurity concerns expressed by government leaders pertain to the security of government networks and so called "critical infrastructure,"[345] such as the electronic power grid and the computer systems controlling power plants, America's telephone networks have not completely escaped the attention of policymakers. Sparked by fears that Chinese communications equipment companies, such as Huawei and ZTE, may have hidden surveillance backdoors in their products at the request of the Chinese government,[346] the U.S. national security establishment responded.[347] According to media reports, both AT&T and Sprint, which had planned to purchase Huawei equipment for their next-generation 4G networks, were threatened by senior officials in the national security community with a consequent loss of government business and the disruption of merger plans.[348] Ultimately, both companies did not purchase Huawei equipment, instead opting for network hardware from Western manufacturers.[349]

Obama Budget Makes Cybersecurity a Growing U.S. Priority, REUTERS (Apr. 10, 2013), http://www.reuters.com/article/2013/04/11/us-usa-fiscal-cybersecurity-idUSBRE93913S20130411 ("Obama's budget, released on Wednesday, proposes to boost Defense Department spending on cyber efforts to $4.7 billion, $800 million more than current levels . . . .").

345. *See, e.g.*, Exec. Order No. 13,636, 78 Fed. Reg. 11739 (Feb. 19, 2013); Presidential Policy Directive — Critical Infrastructure Security and Resilience (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

346. STAFF OF U.S.-CHINA ECON. & SEC. REVIEW COMM'N, THE NATIONAL SECURITY IMPLICATIONS OF INVESTMENTS AND PRODUCTS FROM THE PEOPLE'S REPUBLIC OF CHINA IN THE TELECOMMUNICATIONS SECTOR 7 (Jan. 2011), *available at* http://origin.www.uscc.gov/sites/default/files/Research/FINALREPORT_TheNationalSecurityImplicationsofInvestmentsandProductsfromThePRCintheTelecommunicationsSector.pdf; Jeremy Wagstaff & Lee Chyen Yee, *ZTE Confirms Security Hole in U.S. Phone*, REUTERS (May 18, 2012), http://www.reuters.com/article/2012/05/18/us-zte-phone-idUSBRE84H08J20120518.

347. *See* Antonio Regalado, *Before Snowden, There Was Huawei*, MIT TECH. REV. (Mar. 18, 2014), http://www.technologyreview.com/news/525596/before-snowden-there-was-huawei/ ("[A]nytime [Huawei is near] to closing a sale, their customers get a visit from the FBI or U.S. Department of Commerce. The message from the feds isn't subtle: buy something else."); John Pomfret, *History of Telecom Company Illustrates Lack of Strategic Trust between U.S., China*, WASH. POST (Oct. 8, 2010, 12:33 AM), http://www.washingtonpost.com/wp-dyn/content/article/2010/10/07/AR2010100707210.html ("The message from the NSA . . . was simple: If AT&T wanted to continue its lucrative business with the U.S. government, it had better select a supplier other than Huawei . . . ."); David E. Sanger & Nicole Perlroth, *N.S.A. Breached Chinese Servers Seen as Security Threat*, N.Y. TIMES (March 22, 2014) http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html (noting that "[American officials] have blocked [Huawei] at every turn" and citing three U.S. government intervention against the company).

348. Pomfret, *supra* note 347.

349. *Id.* ("In February, AT&T announced that it would buy the equipment it needed from Swedish-owned Ericsson and Paris-based Alcatel-Lucent."); *see also* Edward Wyatt, *Sprint Nears a U.S. Deal To Restrict China Gear*, N.Y. TIMES (Mar. 28, 2013), http://www.nytimes.com/2013/03/29/business/sprint-and-softbank-near-agreement-to-restrict-use-of-chinese-suppliers.html ("SoftBank and Sprint have already assured members

The House Intelligence Committee also investigated the matter, holding a hearing where executives from both Huawei and ZTE testified. In his opening remarks at that hearing, Committee Chairman Mike Rogers stated that "Americans have to trust our telecommunications networks" and that "[w]hen vulnerabilities in the equipment . . . can be exploited by another country, it becomes a priority and a national security concern."[350] After the hearing, the Committee released a bi-partisan report accusing the companies of collaborating with the Chinese military.[351]

Significantly, when faced with the possibility that U.S. telecommunications networks *might* be vulnerable to exploitation by the Chinese government through security flaws or backdoors, Congress and members of the national security community swiftly examined the problem and took decisive action. In contrast to the resources directed at these Chinese supply chain threats, nothing approaching this kind of effort and focus has been channeled towards other existing security vulnerabilities in our cellular networks that *can* and *are* being exploited by the intelligence services of many countries.

While there are a number of likely reasons why the perceived threat posed by Huawei and ZTE became such a high-profile issue for policymakers, it is worth noting that the "fix" to this problem was rather simple — pressuring major U.S. carriers such as AT&T and Sprint to purchase equipment from Western (thus "trusted") suppliers. The companies that made the mistrusted products are Chinese and thus subject to ready and politically safe (indeed, politically rewarding) demonization by the intelligence community and their allies in Congress. Moreover, the national security threat posed by Chinese government exploitation of backdoors in Chinese telephony equipment, unlike many other threats, offered the inherent political benefit of being legally amenable to public discussion without putting any U.S. government intelligence sources and methods at risk.

In contrast to the Huawei and ZTE threat, the risks posed by the cellular network vulnerabilities described in this Article present a far more politically delicate problem. The technical fix for them may be

---

of Congress that they will not integrate equipment made by Huawei into Sprint's United States systems and will replace Huawei equipment in Clearwire's network.").

350. Rep. Mike Rogers, *Huawei and ZTE Testify Before the House Intel Committee Part 1* at 3:51, 5:53, YOUTUBE (Oct. 3, 2012), http://www.youtube.com/watch?v=ApQjSCUpt4s (recording of testimony before the House Permanent Select Committee on Intelligence on September 13, 2012).

351. *See* CHAIRMAN MIKE ROGERS & RANKING MEMBER C.A. DUTCH RUPPERSBERGER OF H. PERMANENT SELECT COMM. ON INTELLIGENCE, 112TH CONG., INVESTIGATIVE REP. ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE 2, 11 (Oct. 8, 2012), *available at* https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf.

expensive and time-consuming,[352] and the companies that have long known about these vulnerabilities in their networks, yet have neither fixed the vulnerabilities nor warned consumers about the risks, are large, politically active U.S. corporations. Moreover, the devices that exploit these vulnerabilities, which are manufactured by similarly large, politically active defense contractors, are considered sensitive sources and methods that U.S. law enforcement and intelligence agencies would undoubtedly prefer not to be the subject of open discussion at public hearings. It is therefore not surprising that policymakers have failed to tackle this issue, whether in the context of the existing cybersecurity debate or otherwise.

Now that Congress and the FCC have slowly started to acknowledge the national security threats posed by cellular surveillance technology, however, policymakers are likely to look for solutions to the problem. We present and examine some possible solutions next.

IX. PROTECTING OUR COMMUNICATIONS

The cellular communications of billions of people around the world are vulnerable to interception by their own governments, other governments, and tech-savvy criminals. In spite of the determined efforts of the U.S. law enforcement community to suppress disclosure of information about these vulnerabilities and their exploitation by the government, some information has finally entered into public discourse. State legislatures are asking questions about StingRays,[353] members of Congress want to know about their own vulnerability to foreign government surveillance,[354] and the FCC has even created a task force to study various cellular surveillance and cybersecurity threats.[355] The endemic insecurity of U.S. cellular communications

352. *See* Babbage, *supra* note 271. The cost may not be significant if the carriers are already upgrading their networks. *See* E-mail from Karsten Nohl to author (Apr. 21, 2014, 07:03 AM PDT) on file with author ("The biggest cost item is the replacement of old 2G base stations . . . . Sourcing an entire 4G network from non-Chinese suppliers easily adds a few billions to the bill.").

353. Michael Barajas, *HPD Has a Machine that Can Steal Your Phone's Data, Says ACLU*, HOUSTON PRESS (Sept. 23, 2014), http://blogs.houstonpress.com/news/2014/09/hpd_has_a_machine_that_can_steal_your_phones_data.php; John Turk, *Experts Question Transparency of Cell Phone Tracking Device Owned by Sheriff's Office at Legislative Hearing*, OAKLAND PRESS (May 16, 2014), http://www.theoaklandpress.com/general-news/20140516/experts-question-transparency-of-cell-phone-tracking-device-owned-by-sheriffs-office-at-legislative-hearing.

354. *See* Letter from Alan M. Grayson to Tom Wheeler, *supra* note 29.

355. *See* Letter from Tom Wheeler to Alan M. Grayson, *supra* note 302; Craig Timberg, *For Sale: Systems That Can Secretly Track Where Cellphone Users Go Around the Globe*, WASH. POST (Aug. 24, 2014), http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html (stating that the FCC IMSI catcher

networks is now front-page news. This increased attention from the media and policymakers is likely to result in action — whether in the form of legislation, regulation, or merely increased pressure on the cellular industry.

By upgrading the security of their networks, the wireless carriers can protect their customers from some of the cellular interception technologies described in this Article. Such upgrades will be neither cheap nor easy to perform, given the significant size and reach of U.S. cellular networks.[356] Alternatively, consumers' communications could be protected by transitioning to more-secure, Internet-based voice and text communications services that work on top of cellular data and WiFi networks. Or, perhaps, consumers will start to use counter-surveillance technologies capable of detecting nearby cellular surveillance devices. While a thorough examination of the solutions and the regulatory process necessary to execute them is beyond the scope of this Article, this Part will examine a few likely technical avenues through which solutions could come.

A. Securing Cellular Networks

If the wireless carriers and the phones used by their customers exclusively employed modern cellular encryption algorithms, some of the cellular interception vulnerabilities described in this Article would be cured. But the wireless industry has not switched to modern cryptography. Wireless carriers continue to use weak algorithms that were designed in the 1980s and broken in the 1990s.[357] Indeed, the outmoded A5/1 algorithm remains the most widely deployed cellular encryption algorithm in the world.[358] An improved encryption algorithm, A5/3, was developed and standardized by the cellular industry in 2002. A5/3-capable hardware, however, was not built into cellular phones until 2009,[359] and is still not currently used by many carriers.[360] The decade-old A5/3 algorithm, however, may already be

---

task-force has expanded its mission to cover other cellular network security flaws exploited by commercial surveillance technologies).

356. *See* Babbage, *supra* note 271.

357. *See* Green, *supra* note 52 ("GSM is nearly 30 years old. You probably wouldn't blame today's Ford execs for the crash performance of a 1982 Ford Escort, and similarly you shouldn't hold the GSM designers responsible for a 1980s protocol — even if billions of people still rely on it.").

358. *See* Timberg & Soltani, *supra* note 8.

359. *See* Presentation from Harald Welte, *Structural Deficits in Telco Security*, at 19 (Mar. 20, 2012), *available at* https://www.troopers.de/wp-content/uploads/2011/10/TR12_TelcoSecDay_Welte_Mobsec.pdf.

360. *See infra* notes 367–369 and accompanying main text.

showing its age, since it reportedly has already been broken by the NSA and its British counterpart.[361]

Moreover, even though modern smartphones have the capability to communicate using modern, more secure protocols, they must also be able to complete calls and function over older cellular networks where older, weaker encryption is still in use. This necessity for backward compatibility is a source of persistent security vulnerabilities.

By upgrading the encryption algorithms used by existing second generation ("2G") networks or by migrating entirely to more-secure third ("3G") and fourth generation ("4G") technologies, wireless carriers can protect their subscribers from the passive interception vulnerabilities described in Part V.B.[362] Deutsche Telekom ("T-Mobile"), for example, has already upgraded its 2G cellular networks in Germany and four other European countries to A5/3, and has planned similar upgrades in other countries.[363] T-Mobile (U.S.) has quietly begun the process of upgrading the security of its own network.[364] AT&T has apparently opted for a different approach: Rather than upgrading the security of its 2G network, the company has instead committed to shut it down by 2017 in order to repurpose the spectrum for newer 3G and 4G networks.[365] Although AT&T's planned network migration is likely motivated by consumer demand for high-speed data,[366] it will also improve security, because 3G and 4G networks use newer, more secure encryption algorithms.

---

361. Ryan Gallagher, *Operation AURORAGOLD, How the NSA Hacks Cellphone Networks Worldwide*, INTERCEPT (Dec. 4, 2014), https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones ("In 2009, the British surveillance agency Government Communications Headquarters conducted a similar effort to subvert phone encryption . . . using powerful computers to perform a 'crypt attack' to penetrate the A5/3 algorithm, secret memos reveal. By 2011, GCHQ was collaborating with the NSA . . . to attack A5/3 encryption.").

362. More recent cellular phone systems, including 3G and 4G networks, include the capability for phones to authenticate the network base stations. *See generally* Zhang & Fang, *supra* note 52.

363. Press Release, Deutsche Telekom, Deutsche Telekom Upgrades Wiretapping Protection in Mobile Communications (Dec. 9, 2013), *available at* http://www.telekom.com/media/company/210108.

364. *See* Ashkan Soltani & Craig Timberg, *T-Mobile Quietly Hardens Part of Its U.S. Cellular Network Against Snooping*, WASH. POST (Oct 22, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/22/t-mobile-quietly-hardens-part-of-its-u-s-cellular-network-against-snooping/ ("Testing by The Washington Post has found T-Mobile networks using A5/3 in New York, Washington and Boulder, Colorado, instead of the older A5/1 that long has been standard for second-generation (2G) GSM networks in the United States.").

365. *See* Thomas Gryta, *AT&T to Leave 2G Behind*, WALL ST. J. (Aug. 3, 2012, 2:53 PM), http://online.wsj.com/news/articles/SB10000872396390443687504577567313211264588.

366. *Id*. ("With every network generation, the technology becomes more efficient at carrying information. As a result, companies can get better and more profitable usage from shutting down older networks in favor of newer ones, something that AT&T has talked about.").

Protecting telephone subscribers from active surveillance devices is far more difficult, if not practically impossible. Even when a wireless carrier has upgraded their entire network, the telephones used by their subscribers will still connect to networks that use older, insecure networking technology. This backward compatibility, which is a necessary feature in all handsets because any phone might be taken by its owner to rural areas or foreign countries where older networks remain in use, is a vulnerability that can also be exploited for surveillance.[367] Indeed, many of the manufacturers of active surveillance openly advertise the ability to jam 3G and 4G networks in order to force telephones to connect an active interception device masquerading as a 2G base station.[368]

The ability to force modern phones to communicate insecurely is an unintended side effect of the need to maintain compatibility for older, insecure cellular network technologies. As long as phones continue to support older, insecure phone protocols, they can be manipulated into using them, even in cities where all legitimate networks use 3G and 4G technology.

The migration away from 2G, which will be a slow and expensive process for the wireless carriers, will certainly improve the security of cellular networks, but many forms of unmediated surveillance will still be possible. While 3G and 4G networks employ much more secure encryption algorithms that protect calls, text messages, and Internet data from unauthorized interception, sophisticated 4G surveillance devices can still acquire the serial numbers of nearby phones and locate them. Indeed, several law enforcement agencies have already upgraded to the 4G capable Harris Hailstorm, which can locate and identify nearby 4G phones.[369] As the wireless industry slowly mi-

---

367. *See supra* note 52 (discussion of rollback attacks). This is not the only vulnerability that can be exploited in backward compatible phones. An active surveillance device can extract the cryptographic keys associated with particular targeted handsets. This cryptographic key material can then be used to either decrypt call data that had been previously recorded and retained, or used in tandem with a passive interception device to perform real-time interception in the future. *See* ABILITY COMPUTERS & SOFTWARE INDUS. LTD., *supra* note 42.

368. *See 3G UMTS IMSI Catcher*, PKI (last visited Dec. 18, 2014), http://www.pki-electronic.com/products/interception-and-monitoring-systems/3g-umts-imsi-catcher/ ("With our 3G UMTS IMSI Catcher you can redirect single UMTS mobile phones to specific GSM frequencies, in order to monitor the conversation with our active or passive cellular monitoring systems."); *3G-GSM Tactical Interception & Target Location*, GAMMA GROUP, at 40 (2011), *available at* http://info.publicintelligence.net/Gamma-GSM.pdf ("This device will emulate a 3G network to attract 3G mobiles and, for designated Targets, selectively push them to GSM where they remain unless they are rebooted or pushed back to 3G by the GSM system.").

369. *See* Cyrus Farivar, *Cities Scramble To Upgrade "Stingray" Tracking as End of 2G Network Looms*, ARS TECHNICA (Sept. 1, 2014), http://arstechnica.com/tech-policy/2014/09/cities-scramble-to-upgrade-stingray-tracking-as-end-of-2g-network-looms/; Purchase Order, *PIID: DJD13HQG0264*, DRUG ENFORCEMENT AGENCY (Mar. 5, 2014), *available at* http://usaspending.gov/explore?fiscal_year=all&comingfrom=searchresults&

grates away from 2G, many other law enforcement agencies will respond by upgrading from the 2G StingRay to the 4G Hailstorm. For the many state and local law enforcement agencies that presumably only use cellular surveillance devices to identify and track phones, not to intercept communications, the 4G migration will require the purchase of new, expensive surveillance equipment, but ultimately should not impact their technical surveillance capabilities.

Moreover, while 4G surveillance devices are currently very expensive,[370] they will, of course, become cheaper over time and easier for private parties to purchase, as with prior generations of surveillance technology. Indeed, foreign companies are already openly advertising 4G surveillance products.[371] As a result, even though the wireless carriers may eventually be able to protect their customers' communications from unmediated interception, cell phones will likely remain vulnerable to remote identification and tracking, whether by law enforcement agencies, foreign intelligence services, or criminals.

B. "Over-the-Top" Secure Communication Apps

It is possible to deliver secure communications over an insecure network. The HTTPS encryption built into web browsers, which is used to secure data transmitted to and from websites, does just that, enabling someone safely to check her bank balance or to read her email on a public WiFi network where they would otherwise be vulnerable to WiFi interception.[372] Just as the security of Bank of America or Google's websites does not depend on their customers' using secure WiFi networks, so too can the audio and text communications of smartphone users be protected by apps that supply their own encryption, even when the underlying cellular network remains vulnerable to interception.

Smartphone apps already exist, some with hundreds of millions of existing users,[373] which use encryption to protect their users' text,

---

piid=DJD13HQG0264&typeofview=complete ("Sting[R]ay [II] to Hailstorm Upgrade, ETC. the Hailstorm Upgrade is Necessary for the Sting[R]ay System to Track 4g Lte Phones . . . .").

370. *See* Kelly, *supra* note 21 ("The cell-tracking systems [purchased by U.S. law enforcement agencies] cost as much as $400,000, depending on when they were bought and what add-ons they have. The latest upgrade, code-named 'Hailstorm,' is spurring a wave of upgrade requests.").

371. *See 4G/LTE IMSI/IMEI CATCHER*, GSMSOFT (Oct. 3, 2014), http://www.gsmsoft.com.ua/security_4g_ct ("The basic unit of the system is a 4G/LTE module which provides communication with the corresponding types of mobile phones. It also creates a fake BTS (Node B) with the best operation parameters for 4G/LTE communication.").

372. *See* Murphy, *supra* note 256.

373. *See* Mikey Campbell, *Apple Sees 2 Billion iMessages Sent Daily from Half a Billion iOS Devices*, APPLE INSIDER (Jan. 23, 2013) http://appleinsider.com/articles/13/01/23/apple-sees-2b-imessages-sent-every-day-from-half-a-billion-ios-devices; Derek Snyder, *Skype*

voice, and video communications as they are transmitted over the Internet. Examples of such apps include Microsoft's Skype,[374] Apple's FaceTime and iMessage,[375] Google's Hangouts[376] and Facebook's WhatsApp.[377] These apps use the cellular data network, rather than the wireless carriers' legacy voice and text message systems, to transmit content. In many cases, these are available as third-party apps that individuals must download from an app store. However, smartphone operating system companies including Apple and Google pre-install their own communications apps on devices running their respective operating systems. In some cases, these apps are even enabled by default and seamlessly encrypt communications without requiring any configuration by the user.[378]

Passes 100M Android Installs and Launches Redesigned 4.0, SKYPE BIG BLOG (July 1, 2013), http://blogs.skype.com/2013/07/01/skype-passes-100m-android-installs-and-launches-redesigned-4-0/; Daisuke Wakabayashi, *Cook Raises, Dashes Hopes for Excitement at Apple Annual Meeting*, WALL ST. J. (Feb. 28, 2014), http://blogs.wsj.com/digits/2014/02/28/cook-raises-dashes-hopes-for-excitement-at-apple-annual-meeting/ ("Apple said it sends 'several billion' messages on its iMessage service every day. Apple said users also send 15 million to 20 million FaceTime messages every day.").

374. *Frequently Asked Questions — Does Skype Use Encryption*, SKYPE (last visited Dec. 13, 2014), https://support.skype.com/en/faq/FA31/does-skype-use-encryption ("All Skype-to-Skype voice, video, file transfers and instant messages are encrypted. This protects you from potential eavesdropping by malicious users."). *But see* Glenn Greenwald et al., *Microsoft Handed the NSA Access to Encrypted Messages*, GUARDIAN (July 12, 2013), http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (revealing that Skype was served "with a directive to comply signed by the attorney general" and the NSA has since been able to intercept Skype video and audio communications).

375. *See We've Built Privacy into the Things You Use Every Day*, APPLE (last visited Dec. 18, 2014), http://www.apple.com/privacy/privacy-built-in/ ("Your communications are protected by end-to-end encryption across all your devices when you use iMessage and FaceTime . . . . Apple has no way to decrypt iMessage and FaceTime data when it's in transit between devices . . . and we wouldn't be able to comply with a wiretap order even if we wanted to.").

376. *How Hangouts Encrypts Information*, GOOGLE (last visited Dec. 18, 2014), https://support.google.com/hangouts/answer/6046115?hl=en.

377. *See* Ellen Nakashima, *WhatsApp, Most Popular Instant-Messaging Platform, To Encrypt Data for Millions*, WASH. POST (Nov. 18, 2014), http://www.washingtonpost.com/world/national-security/whatsapp-worlds-most-popular-instant-messaging-platform-to-encrypt-data-for-millions/2014/11/18/b8475b2e-6ee0-11e4-ad12-3734c461eab6_story.html ("Open Whisper Systems, a group of software developers, said Tuesday it had partnered with Silicon Valley's WhatsApp to build in end-to-end encryption that will make it impossible for foreign governments and U.S. agencies to intercept text messages, even with a warrant."); Andy Greenberg, *WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users*, WIRED (Nov. 18, 2014), http://www.wired.com/2014/11/whatsapp-encrypted-messaging/ ("The result is practically uncrackable encryption for hundreds of millions of phones and tablets that have Whats[A]pp installed — by some measures the world's largest-ever implementation of this standard of encryption in a messaging service.").

378. For example, since 2011, Apple's iOS operating system has used its own iMessage service for all text messages sent between iOS devices. Such text messages are, without requiring any configuration or special action by the user, encrypted and sent over the Internet using Apple's servers, rather than using the wireless carrier's text message servers. *See* Andy Greenberg, *Apple Claims It Encrypts iMessages and Facetime so That Even It*

Communications made using these apps cannot be intercepted using the surveillance devices discussed in this Article. Moreover, some services, such as Apple's iMessage and FaceTime, Facebook's WhatsApp, and a few other third-party apps that encrypt messages end-to-end, protect against interception not only by wireless carriers and, Internet Service Providers, but also by the companies that provide these apps.[379] Indeed, end-to-end encryption technology protects the contents of user communications from interception by all but the most skilled actors.[380]

Even so, most of these apps, particularly those made by the largest technology companies, do not openly advertise the security advantages of their services. Instead, they typically compete on cost or ease of use. Once the ease with which cellular communications can be intercepted becomes known to more consumers, however, those companies with widely used communications apps are well-placed to compete and deliver a more secure communications experience to consumers.

C. Counter-Surveillance Technology

The FBI, which acts as the national coordinator for law enforcement use of cellular surveillance technology,[381] has insisted that information about the technology must be kept secret to avoid "provid[ing] adversaries with critical information . . . necessary to develop defensive technology, modify their behaviors and otherwise take countermeasures designed to thwart the use of this technology."[382] It may be too late. Indeed, some of the biggest players in the cellular surveillance market have already sought patents, and thus filed public applications describing, in significant detail, techniques

---

Can't Decipher Them, FORBES (June 17, 2013), http://www.forbes.com/sites/andygreenberg/2013/06/17/apple-claims-it-encrypts-imessages-and-facetime-so-that-even-it-cant-read-them/; Greenberg, *supra* note 377 (describing the implementation of WhatsApp's new encryption scheme as "totally frictionless").

379. *See We've Built Privacy into the Things You Use Every Day*, *supra* note 375; Nakashima, *supra* note 377.

380. Even when communications are encrypted, it is still possible for a determined adversary (such as a law enforcement or intelligence agency) to intercept those communications. By infecting the end-point (such as a mobile phone or laptop used by one of the callers) with specially designed surveillance software, sophisticated actors can obtain unencrypted audio, video, and text communications from a target's device. U.S. law enforcement and intelligence agencies already use such software. *See* Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics To Spy on Suspects*, WALL ST. J. (Aug. 3, 2013), http://online.wsj.com/news/articles/SB10001424127887323997004578641993388259674 ("The FBI develops some hacking tools internally and purchases others from the private sector. With such technology, the bureau can remotely activate the microphones in phones running Google Inc.'s Android software to record conversations . . . . It can do the same to microphones in laptops without the user knowing . . . .").

381. *See* FCC REPORT AND ORDER, *supra* note 9.

382. Morrison Affidavit 2014, *supra* note 174.

that can detect active cellular surveillance devices.[383] Although it is unlikely that these companies will sell their counter-surveillance products to the general public, there are now a number of other ways for individuals to acquire software or devices capable of detecting cellular surveillance technology.

Over the past several years, several academic researchers and boutique security companies have created their own "IMSI catcher catcher" counter-surveillance products. The first public project, which was released by researchers in 2011, was extremely difficult to use, requiring the user to replace the operating system on a widely available $15 Motorola phone with custom software.[384] According to the researchers who developed the software, IMSI catchers show different behavior from normal base stations to achieve their goals. The software "distinguish[es] between yellow, red, and black flags. Yellow flags are an indication that you might have been caught; red flags are a very strong indication; and black flags tell you: 'You are being tracked down; throw away your phone and run.'"[385] A few years later, a different team of researchers released an Android app for the popular Samsung Galaxy S3 smartphone capable of detecting IMSI catchers. In contrast to the earlier effort, use of this app did not require that the user replace their entire phone operating system.[386] The app is available from Google's App Store, and can be easily installed by anyone in just a few steps.[387]

In spite of the FBI's efforts, the tools and information necessary to detect cellular surveillance devices are now public. Academics have published peer-reviewed research describing novel techniques to detect cellular surveillance,[388] MIT students in 2014, as a class project, built their own counter-surveillance app,[389] and boutique security

383. *See* Jeffrey F. Bull & Matthew L. Ward, *Interference Detection, Characterization and Location in a Wireless Communications or Broadcast System*, GOOGLE (Dec. 11, 2009), https://www.google.com/patents/WO2010077790A1; Eithan Goldfarb, *Systems and Methods for Identifying Rogue Base Stations*, GOOGLE (Apr. 30, 2013), https://www.google.com/patents/EP2661113A1.

384. *See* Krempl, *supra* note 226; *CatcherCatcher*, SECURITY RESEARCH LABS (last visited Dec. 18, 2014), https://opensource.srlabs.de/projects/mobile-network-assessment-tools/wiki/CatcherCatcher.

385. *See CatcherCatcher*, *supra* note 384.

386. *See* Ravishankar Borgaonkar, *Understanding IMSI Privacy*, BLACKHAT USA 2014 (Aug. 7, 2014), https://www.isti.tu-berlin.de/fileadmin/fg214/ravi/Darshak-bh14.pdf; *Darshak*, GITHUB (last visited Dec. 18, 2014), https://github.com/darshakframework/darshak/.

387. *See Darshak*, GOOGLE PLAY (last visited Dec. 18, 2014), https://play.google.com/store/apps/details?id=com.darshak&hl=en.

388. *See* Adrian Dabrowski et al., *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers*, *in* ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE (ACSAC) 2014 (Dec. 8–12, 2014), *available at* https://www.sba-research.org/wp-content/uploads/publications/AdrianDabrowski-IMSI-Catcher-Catcher-ACSAC2014-preprint-20140820.pdf.

389. *See* Jeffrey Warren, *ACLU + the Guardian Project Final Project*, CODESIGN (May 18, 2014), http://codesign.mit.edu/2014/05/aclu-the-guardian-project-final-project/.

companies now openly sell, to the general public, surveillance-resistant smartphones with built-in counter-surveillance features.[390] Although, for now, such features are not built into the popular Android and Apple smartphones that most consumers use, they may be in the future as big Silicon Valley technology companies begin to compete openly on privacy and security.[391]

X. CONCLUSION

This Article has illustrated how cellular interception capabilities and technology has become, for better or worse, globalized and democratized, placing Americans' cellular communications at risk of interception by foreign governments, criminals, and the tabloid press, to mention a few. Notwithstanding this risk, U.S. government agencies shroud almost every aspect of the StingRay and similar direct interception technology in secrecy, in an ostensible but futile effort to prevent criminals from learning how to thwart the technology. But this narrative, which disingenuously asserts a continuing need for secrecy regarding StingRay technology, does greater harm by inhibiting public awareness and discussion of the risks associated with private use of unmediated surveillance technologies, thus preventing policymakers from addressing the underlying vulnerabilities in cellular networks. Those who cling to the position that a demonstrably illusory veil of secrecy is essential to protect the utility of surveillance capabilities, and who, as a consequence, suppress information necessary to a full public discussion of cellular network security, effectively undermine broader congressional efforts to strengthen cybersecurity. This unnecessary and counterproductive veil must be lifted so that the public and legislators can address the full scope of interception risks in a public policy process that will promote better, stronger cybersecurity practices.

---

390. *E.g.*, *Cryptophone*, GSMK (last visited Dec. 18, 2014), http://www.cryptophone.de/; *Stealth Phone*, X-CELLULAR (last visited Dec. 18, 2014), http://x-cellular.com/phones.html.

391. *See* Craig Timberg, *Apple Will No Longer Unlock Most iPhones, iPads for Police, Even with Search Warrants*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/business/technology/2014/09/17/2612af58-3ed2-11e4-b03f-de718edeb92f_story.html; Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/; Matthew Green, *Is Apple Picking a Fight with the U.S. Government? Not Exactly*, SLATE (Sept. 23, 2014), http://www.slate.com/articles/technology/future_tense/2014/09/ios_8_encryption_why_apple_won_t_unlock_your_iphone_for_the_police.html ("Apple is not designing systems to prevent law enforcement from executing legitimate warrants. It's building systems that prevent everyone who might want your data — including hackers, malicious insiders, and even hostile foreign governments — from accessing your phone.").