MEDIA FIELDS
JOURNAL

Rise of the IMSI Catcher

Lisa Parks

In the wake of the Patriot Acts and the Snowden revelations, new details about surveillance technologies rarely seem surprising. Many have grown accustomed to Constitution-violating "sneak and peek" search warrant practices, biometric scanning, and sensors that make anything and everything monitor-able, no matter how large or small. As billions of people around the world are becoming digitally connected, the Kool-Aid is beginning to wear off. Networked office workers are revolting against the constant scrutiny of their online activities. Internet users are upset that Twitter and Facebook are in cahoots with the National Security Agency (NSA). And GPS-equipped smartphones seem more and more like electronic ankle bracelets. The utopian allure of connectivity is cracking and totalitarian tendencies are alive and kicking, especially in the world's democracies.

Such conditions have kept surveillance scholars busy. Since 9/11, scholars have analyzed the monumental shifts in surveillance that have unfolded in the context of the War on Terror.[1] They have demonstrated that digital networks and social media have become havens for state and corporate monitoring of citizens' expressions and transactions.[2] They have explored how techniques of racial profiling, biometrics, and physical searching continue to disenfranchise people who are already vulnerable or immersed in struggles for social equality and justice, including the poor, people of color, and refugees.[3] And they have charted the labyrinthine expansion of closed-circuit and airport security systems and the complex dynamics of their use.[4] Despite the plethora of vital topics that have been tackled, surveillance

scholars have yet to discuss a gadget of growing concern—a cellphone interception technology known as the IMSI catcher.[5]

Also called a "man-in-the-middle" device, "cell site simulator," "StingRay," and "dirtbox," the IMSI (International Mobile Subscriber Identity) catcher functions by simulating a cellphone base station. It locks on to cellphones in a given vicinity and then intercepts data from and/or remotely reconfigures or operates the phones. Because of the powerful surveillance capability it provides, it has been incorporated into the work of military units, state agencies, law enforcement agencies, spies, hackers, and criminal organizations. Yet, the devices were relatively secret until recently, because organizations have used them surreptitiously and some manufacturers have required their clients to sign non-disclosure agreements that forbid public discussion of the technology's use.[6] Over the past decade, a series of lawsuits was filed in connection with IMSI catcher use and civil rights organizations and journalists began to ask questions. Hackers also began to figure out how to build and detect the devices. At the same time, more manufacturers entered the market, new models proliferated, and the price of IMSI catchers dropped dramatically. The IMSI catcher is now part of a lawful interception industry that is expected to be worth $1.3 billion by 2019, up from $251 million in 2014.[7] In short, cellphone interception could become as common as cellphone use.

In an effort to encourage further work on the IMSI catcher, this essay provides a broad overview of the technology's emergence, manufacturers, and uses in different parts of the world. The essay concludes with a discussion of critical issues elicited by its proliferation and use and suggests avenues for further research.

Making the Man-in-the-Middle

While telephone interception technology dates back to the late 19th century, the IMSI catcher first emerged in the early 1990s.[8] The first publicly known companies to manufacture and sell them were based in Germany and Israel. Rohde & Schwarz, a major German electronics manufacturer founded in 1933, presented its first IMSI catcher in 1996 in Munich. Model GA 090 was designed to identify a cellphone subscriber by accessing the phone's IMSI—a number that is unique to every SIM card—and then determining the subscriber's phone number with help from the network operator. GA 900, a later model released in 1997, enabled the user to also tap outgoing cellphone

calls.[9] Rohde & Schwarz now has 9900 employees and operates in 70 countries. Another German company called PKI now markets multiple IMSI catchers as "Anti Terror Equipment" and even runs its own training facility.[10]

Leading Israeli manufacturer, Ability, was formed in 1993 to design interception and decryption devices. Under the motto "Forewarned is forearmed," the company currently sells five cellphone interception systems and a device called the IBIS Airborne II that attaches to aircraft.[11] A promotional video describes the machine as one that "takes cellular interception to a higher level."[12] The narrator explains that the IBIS Airborne II undetectably intercepts information from cellphones and tracks their locations in real time from a plane flying overhead.[13] Reflecting the nebulous boundaries between surveillance and counter-surveillance, Rayzone Corporation, a newer Israeli company founded in 2010, makes both an IMSI catcher called Piranha and an IMSI catcher *detector* called ArrowCell.[14]

Figure 1 The Sting Ray

In the United States, the Florida-based Harris Corporation has been a primary manufacturer of IMSI catchers. Its devices, branded as StingRays, were first developed for the military and intelligence agencies. The company registered the original trademark in 2001 and sold the StingRay for $65,479. The more powerful StingRay II, released between 2007 and 2008, was priced at $134,952.[15] Harris Corporation now sells a full fleet of cellphone interceptors with names like Gossamer, Triggerfish, Amberjack, and Harpoon. They have different features and technical abilities, come in various sizes, and can cover a range of distances. One of its newest models,

Hailstorm, can even remotely inject malware into cellphones.[16] Another US company, Digital Receiver Technology, Inc. (DRT), a Boeing subsidiary, is known for its manufacture of DRTBOX ("dirtbox"). This device costs $78,850 and can be installed on planes to scan phones on the ground.[17] US-based Meganet Corporation makes the VME Dominator, which offers "voice manipulation, up or down channel blocking, text intercept and modification, calling & sending text on behalf of the user, and directional finding of a user during random monitoring of calls."[18] Finally, the Gamma Group has developed car-integrated and body-worn IMSI catchers.[19]

Given the increasing demand for and the ease of assembling the technology, IMSI catchers are now being produced in various parts of the world, including China. On Alibaba.com—the Chinese equivalent of Amazon.com—a search for "imsi catcher" in February 2016 turned up 270 related products and 31 Chinese suppliers such as Shenzhen TYH Technology Co., LTD, Telepower Communication, and Shenzhen Etross Telecom Co., Ltd.. Models range in capacity, and prices average between $1200-2050, though some components cost as little as $50 and one device was selling for $30,000. Presumably to attract global sales, some IMSI catcher product taglines include phrases such as "Hot product in Dubai" or "Nigeria new security system." Their listings sometimes also feature illustrated use scenarios, technical instructions, or photos of women working on the manufacturer's assembly lines.[20]

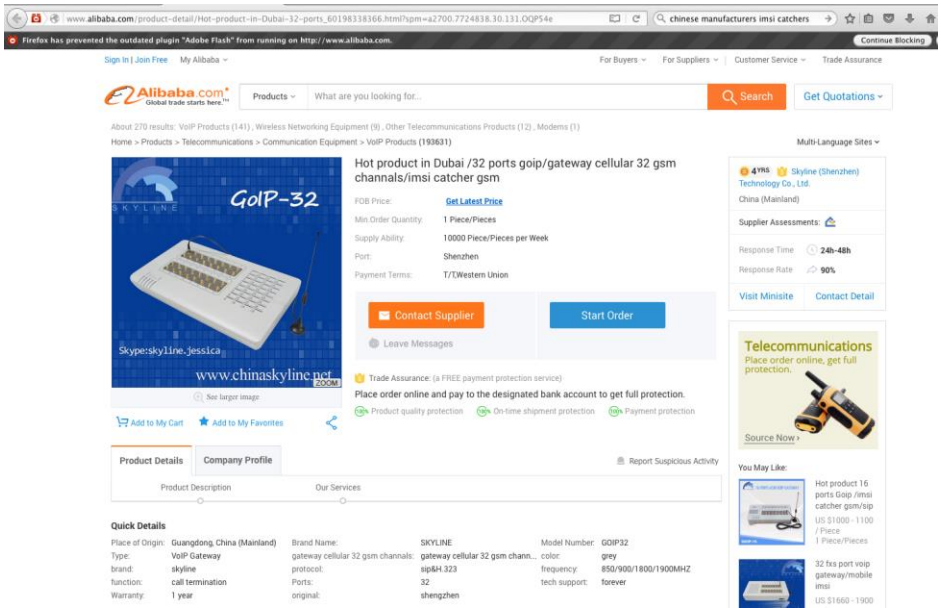

Figure 2 IMSI Catcher - Hot Product in Dubai

Until recently, public information about IMSI catcher manufacturers and their devices was relatively limited. In December 2015, *The Intercept* acquired and published a secret internal US government catalogue of cellphone surveillance devices used by the military and intelligence agencies. The catalogue provides details on manufacturers and their product lines, and identifies vendors such as the NSA and the Central Intelligence Agency (CIA). According to *The Intercept*, "Nearly a third of the entries focus on equipment that seems to have never been described in public before."[21] The original document is formatted as if ready-made for inclusion in PowerPoint presentations, with photos of each device and lists of its capabilities, limitations, planning factors, and price. The catalogue includes StingRays and dirtboxes as well as a $9920 machine called CellBrite, which, *The Intercept* claims, will "suck every last byte of data out of a seized cellphone."[22] Each page of the May 1, 2006 document is marked "SECRET//NOFORN," a distribution criterion for US classified materials that means "No Foreign Nationals." Each page is also stamped with a January 7, 2034 declassification date, which suggests that these devices are likely to be around for a while.[23]

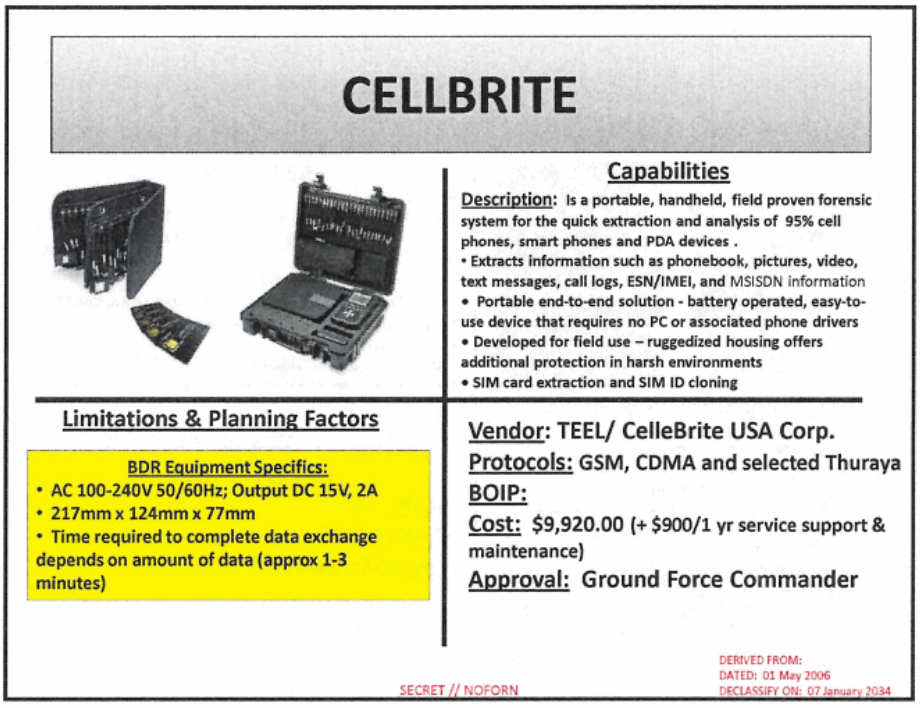

Figure 3 The CellBrite

In the last several years, ad hoc groups, hackers, and researchers have built their own IMSI catchers, some in the spirit of the open-source movement. Multiple press reports refer to Chris (now Kristen) Paget's 2010 DEFCON presentation "Practical Cell Phone Spying." In that talk, Paget demonstrated a $1500 homemade system constructed from software-defined radio and free open-source software such as GNU Radio, OpenBTS, or Asterisk.[24] Another report indicates that a team was able to convert a Verizon cell network extender into an IMSI catcher that fit into a backpack.[25] And in 2015, a research group from Helsinki and Berlin combined $1400 worth of hardware with open-source software to create its own IMSI catcher. That device works on newer 4G/LTE networks and tracks a phone's precise location by using signals from Facebook and WhatsApp messengers.[26] What was once a highly secret technology is becoming more widely known. One security expert describes the situation as the "democratization of Stingray,"[27] while legal analysts suggest that we are on the brink of an era in which everyone can eavesdrop on cellphone conversations.[28]

Surveillance, Spying, and Spam

Cases of IMSI catcher use have been reported around the world, including in the US, United Kingdom, Norway, South Africa, Ukraine, China and India.[29] In the US, law enforcement officers have used cellphone simulators since 1995 and adopted the use of StingRays around 2003.[30] Information about the technology began to circulate publicly due to high-profile legal decisions, in connection with tax fraud (*United States v. Rigmaiden* in 2011-2013) and drug trafficking (a Texas federal magistrate judge denying the Drug Enforcement Agency's use of a StingRay in 2012).[31] In the former case, law enforcement officers used IMSI catchers to intercept cellphone data that led to the target's arrest and prosecution. In the latter case, federal agents in the pursuit of a suspect ran up against a rare instance of judicial restriction. Organizations such as the American Civil Liberties Union (ACLU), Electronic Frontier Foundation (EFF), and Electronic Privacy Information Center (EPIC) have followed these developments closely. Controversies have arisen in several cases as law enforcement officers refused to testify about their use of IMSI catchers. They cited the non-disclosure agreement the Harris Corporation required them to sign, noting that it forbids public discussion of the technology.[32]

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

Serial Description ~ Unrecorded Serial

Total Deleted Page(s) ~ 481
Page 2 ~ b3, b4, b7E
Page 3 ~ b3, b4, b7E
Page 4 ~ b3, b4, b7E
Page 5 ~ b3, b4, b7E
Page 6 ~ b3, b4, b7E
Page 7 ~ b3, b4, b7E
Page 8 ~ b3, b4, b7E
Page 9 ~ b3, b4, b7E
Page 10 ~ b3, b4, b7E
Page 11 ~ b3, b4, b7E
Page 12 ~ b3, b4, b7E
Page 13 ~ b3, b4, b7E
Page 14 ~ b3, b4, b7E
Page 15 ~ b3, b4, b7E
Page 16 ~ b3, b4, b7E
Page 17 ~ b3, b4, b7E
Page 18 ~ b3, b4, b7E
Page 19 ~ b3, b4, b7E
Page 20 ~ b3, b4, b7E
Page 21 ~ b3, b4, b7E
Page 22 ~ b3, b4, b7E
Page 23 ~ b3, b4, b7E
Page 24 ~ b3, b4, b7E
Page 25 ~ b3, b4, b7E
Page 26 ~ b3, b4, b7E
Page 27 ~ b3, b4, b7E
Page 28 ~ b3, b4, b7E
Page 29 ~ b3, b4, b7E
Page 30 ~ b3, b4, b7E
Page 31 ~ b3, b4, b7E
Page 32 ~ b3, b4, b7E
Page 33 ~ b3, b4, b7E
Page 34 ~ b3, b4, b7E
Page 35 ~ b3, b4, b7E
Page 36 ~ b3, b4, b7E
Page 37 ~ b3, b4, b7E
Page 38 ~ b3, b4, b7E
Page 39 ~ b3, b4, b7E
Page 40 ~ b3, b4, b7E
Page 41 ~ b3, b4, b7E
Page 42 ~ b3, b4, b7E
Page 43 ~ b3, b4, b7E
Page 44 ~ b3, b4, b7E
Page 45 ~ b3, b4, b7E

XXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X for this Page X
XXXXXXXXXXXXXXXXXXXXXXXX

Figure 4 FOIPA Deleted Page Information Sheet

A 2012 EFF investigation of IMSI catcher use in the US found "hundreds of thousands of searches for cell phone location information" and the "skyrocketing of warrantless surveillance."[33] In February 2012, EPIC submitted a Freedom of Information Act (FOIA) request to the Federal Bureau of Investigations (FBI). It sought technical details about StingRays and cellphone simulators, as well as the Bureau's procedures and legal rationales for using them.[34] The FBI responded to the FOIA request with 13 releases of 20,000 largely redacted documents between October 2012 and July 2013. The nature of the reply made the agency's commitment to suppressing information about the technology particularly evident.[35] Ironically, it is possible to find more technical information about IMSI catchers on Alibaba.com than through these 20,000 pages of federal documents.

Given the broad authorizations of the Patriot Acts (not to mention law enforcement officers' physical seizures of suspects' cellphones[36]), IMSI catcher use in the US is hardly surprising. However, it is worth noting that the publicized instances of the device's use have been linked to the prosecution of tax evaders and drug traffickers rather than terror suspects. It remains to be determined if and how IMSI catchers are being used in practices of racial, religious, and neighborhood profiling. For instance, how often are IMSI catchers used to monitor the cellphone activity of Arab and Muslim Americans, residents in urban Black communities, or visitors entering the US from particular countries? How are IMSI catchers deployed along the US-Mexico border? The specific ways that cell site simulators support racist surveillance practices have yet to be fully investigated. Yet, there have already been reports of IMSI catcher use during Black Lives Matter protests in Minneapolis and Chicago.[37] Anonymous made a video about the Chicago incident that featured audio feeds from a Chicago Police Department fusion center.[38] And the Baltimore Police Department has reportedly used cellphone simulators to track 4300 phones since 2007.[39] The growing use of IMSI catchers in the US led Representative Jason Chaffetz of Utah to introduce a Congressional bill called the Cell-Site Simulator Act of 2015 that would prevent government agencies from using StingRays without a warrant in most conditions.[40]

In India, IMSI catchers have been used as tools of industrial espionage. Private companies and individuals allegedly smuggled an estimated 2000 IMSI catchers into India (made in Israel, China, the UK, France, and Sweden) through Nepal and Bangladesh, and used the devices illegally to intercept

cellphone conversations.[41] Over 90% of the devices were imported by the private sector. The devices cost approximately 18,000 rupees (about $350) and could record 10-12 conversations simultaneously within a 2-kilometer radius. In an attempt to eradicate their private-sector use, the Indian government banned IMSI catchers in 2012. It also created a period in which the devices could be turned over to the government without prosecution, but none were presented. In the Indian case, the IMSI catcher has become part of an intensely competitive entrepreneurial culture, in which companies exploit any strategic advantage to succeed in the marketplace.

In China, IMSI catchers have been used to disseminate spam. In 2014, Chinese authorities arrested more than 1500 people for sending spam text messages through illegal fake mobile phone base stations. Authorities reportedly seized more than 2600 of these stations and shut down 24 sites where IMSI catchers were illegally manufactured. China's Ministry of Public Security reported more than 3500 cases of suspected crimes related to the technology.[42] News reports about the use of these devices in China have emphasized the illegal spam incident, but states can also use the technology to track political dissidents, journalists, activists, ethnic or sexual minorities, and foreigners. As evidence of the broader use of the technology in China, one security expert claims that four Chinese airlines use IMSI catchers to spy on passengers.[43]

Indeed, there is growing concern about IMSI catcher use both in democracies and authoritarian regimes. While authoritarian regimes typically nationalize and maintain control of their mobile telephone operators, the IMSI catcher makes interception of cellphone data more efficient, discrete, and immediate. As one security expert contends, "At this point, every dictator in the world is using this technology against its own citizens."[44] While this may be true, it is difficult to find public confirmation of such facts. Thus far, civil rights organizations and investigative journalists have taken the lead in ascertaining where and how IMSI catchers are used. For instance, Privacy International gained access to Swiss export records that indicated the distribution of IMSI catchers to Ethiopia, Indonesia, Qatar, Kuwait, Lebanon, Lithuania and Thailand in 2014 for a total cost of 5.2 million pounds (about $7.5 million). The sale of the devices across multiple continents suggests that state use is quite widespread.[45] The ACLU has also mapped IMSI catcher deployment in states across the US and provided a list of all known agencies that use them.[46]

Cat and Mouse

As IMSI catcher use proliferates, so do counter-responses to it. Such is the game of cat and mouse that characterizes technical innovation in the surveillance sector. Indeed, several IMSI catcher detection devices have already emerged. Publicly known counter-responses include the IMSI Catcher Catcher, which Karsten Nohl developed in 2007; Snoop Snitch, an Android app available on Google Play that Nohl's German-based Security Research Labs created in 2014; and AIMSICD (Android IMSI Catcher Detector), an app that a group of self-described "privacy-minded folks" began to develop in 2012.[47] In addition to these projects, ESD America's $3500 GSMK CryptoPhone 500i is capable of IMSI catcher detection.[48] Research groups in Europe and the US are also currently developing other cell site simulator detection systems.[49]

IMSI catcher use raises a host of critical issues, of which I have only scratched the surface here, but I want to close by briefly discussing three points. First, there is a tendency in surveillance studies to adopt a position of cynicism in relation to the post-9/11 expansion of surveillance. Such a stance assumes that state surveillance is a *fait accompli* and that little can be done to combat it. The popularization of the phrase "nothing to hide" ultimately reinforces this cynical position and, in effect, authorizes warrantless searching. The logic of this position is something like, "I know you're going to search anyway, so go ahead. You won't find anything illegal. I have nothing to hide." Operating within such a mentality is problematic because it wrongly assumes that everyone is treated equally under the gaze of surveillance. The point here is that cynicism—the idea that "we are all being watched all the time anyway"—can only sustain a vague level of critique that reifies existing conceptions of observation (such as Big Brother or the panopticon). It neglects the dynamic particularities of surveillance technologies, as well as their multifarious uses and embodied affects. Further earnest, roll-up-your-sleeve research on the socio-technical, political, economic, and historical aspects of surveillance technologies is needed to generate salient new theories of surveillance and power.

Second, when it comes to the international diffusion of surveillance technologies like the IMSI catcher, paternalistic posturing often takes shape. Western liberals often assume that democratic nation-states are able to develop and use surveillance technologies "responsibly" because they have Constitutions, checks and balances, and the rule of law. According to this

logic, real problems only occur and people are only truly oppressed when *authoritarian regimes* deploy surveillance devices. Such an assumption is not only blind to the history of surveillance in Western democracies and its continuing uses against ethnic minorities; it also neglects the fact that many democracies flagrantly displaced their Constitutions in the name of counterterrorism after 9/11. In the US, the Patriot Acts have fundamentally changed law enforcement culture by broadening the definition and scope of legitimate and authorized searches, sometimes referred to as "function creep." Given such developments, the argument that a rule of law serves as an important check on state surveillance power no longer holds, if it ever did. As Anthony Giddens powerfully argued thirty years ago, both Western democracies and authoritarian regimes have used surveillance technologies in totalitarian ways.[50] The globalization of the IMSI catcher not only provides opportunities for the transnational study of surveillance in the age of the cellphone; it also demands a deeper analysis of "lawful interception" in Western democracies where use of the technology originated and is becoming more widespread. The recent terrorist attacks in Paris and San Bernardino, combined with the influx of refugees into Germany and other parts of Europe, is bound to intensify and expand IMSI catcher use in Western democracies. Tracking how the technology is used in such contexts is a critical research agenda.

Video 1 Phone Hackers

Finally, one of the most troubling aspects of the IMSI catcher's emergence has been the suppression of information around its use. To uphold Constitutional rights, it is essential that law enforcement agencies provide details about the surveillance technologies they use. They must also proffer evidence that they abide by the policies that circumscribe the use of such technologies. This means that the rise of the IMSI catcher is necessarily bound up in issues of technological literacy and the politics of knowledge. It is impossible to protect civil liberties if citizens remain unaware of the technical potential to undetectably intercept their cellphone data. To expand public knowledge of cell site simulators, a video called "Phone Hackers: Britain's Secret Surveillance" features a news crew trying to ascertain whether the technology was used during a demonstration in London.[51] The team wanders around the city, shifting attention between cell tower sites and a laptop running an IMSI catcher detection system. In the process, the team asks several police officers if they are aware of the technology, all of whom refuse to speak about it. The project compellingly reveals that the detection of cell site simulators is contingent upon a knowledge of cellphone infrastructure. Technological literacy is a crucial dimension of surveillance and counter-surveillance. The video also enacts what I have called elsewhere an "infrastructural disposition" by staging encounters with cell tower sites and spectrum activity and publicizing details about their material properties and capacities[52]. If, as reports suggest, IMSI catchers have been found mounted on the light poles of defense firms' parking lots in Washington DC; in Palo Alto, the capital of Silicon Valley;[53] at Black Lives Matters protests in Chicago; and in the Anaheim skies above Disneyland, then further investigative and site-specific research are needed to understand the rise of the IMSI catcher and the politics of its uses.

Author's note: I am grateful to Daniel Grinberg and Lisa Han for helpful research and editorial assistance.

Notes:

1. See, for instance, David Lyon, *Surveillance after September 11* (Cambridge, UK and Malden, MA: Polity Press, 2003); Armand Mattelart, *The Globalization of Surveillance* (Cambridge, UK and Malden, MA: Polity Press, 2010); Louise Amoore, "Biometric Borders: Governing mobilities in the war on terror," *Political Geography* 25, no. 3 (2006): 336-351; Didier Bigo, "Globalized (in)security: the field and the ban-opticon" in *Terror, Insecurity and Liberty: Illiberal practices of liberal regimes after 9/11*, eds. Didier Bigo and Anastassia Tsoukala (New York and London: Routledge, 2008), 10-48; Torin Monahan, *Surveillance in the Time of Insecurity* (New Brunswick, NJ: Rutgers University Press, 2010); Zygmunt Bauman and David Lyon, *Liquid Surveillance* (Cambridge, UK and Malden, MA: Polity Press, 2012); David Lyon, *Surveillance after Snowden* (Cambridge, UK and Malden, MA: Polity Press, 2015).
2. Mark Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (Lawrence, KS: University of Kansas Press, 2007); Anders Albrechtslund, "Online Social Networking as Participatory Surveillance," *First Monday* 13, no. 3 (2008), http://journals.uic.edu/ojs/index.php/fm/article/view/2142/1949; Alice Marwick, "The Public Domain: Social Surveillance in Everyday Life," *Surveillance & Society* 9, no. 4 (2012): 378-393; Daniel Trottier, *Social Media as Surveillance, Rethinking Visibility in a Converging World* (Farnham, UK and Burlington, VT: Ashgate, 2012); eds. Christian Fuchs et al., *Internet and Surveillance: The Challenges of Web 2.0 and Social Media* (New York and London: Routledge, 2012).
3. See Kelly Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York: New York University Press, 2011); Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Durham, NC and London: Duke University Press, 2015); Rachel E. Dubrofsky and Shoshana Amielle Magnet, eds. *Feminist Surveillance Studies* (Durham, NC and London: Duke University Press, 2015).
4. Gavin J.D. Smith, *Opening the Black Box: The Work of Watching* (New York and London: Routledge, 2014); Mark B. Selter, ed., *Politics at the Airport* (Minneapolis: University of Minnesota Press, 2008); Rachel Hall, *The Transparent Traveler: The Performance and Culture of Airport Security* (Durham, NC and London: Duke University Press, 2015).
5. In this essay, I use "IMSI catcher" as a general term for devices that simulate cell phone base stations to intercept cell phone data or

remotely control cell phones. These devices are also known as "cell site simulators," among other names.

6. 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/.
7. "Lawful Interception Market worth $1,342.4 million by 2019," *Markets and Markets*, press release, http://www.marketsandmarkets.com/PressReleases/lawful-interception.asp
8. See, for instance, Phil Lapsley, *Exploding the Phone: The Untold Story of the Teenagers and Outlaws Who Hacked Ma Bell* (New York: Grove Press, 2013); Brian Hochman, *All Ears: A History of Wiretapping in the United States*, forthcoming
9. Daehyun Strobel, "IMSI Catcher," Seminararbeit Ruhr-Universität Bochum, July 13, 2007, https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf.
10. "Active GSM Monitoring System with IMSI Catcher and Decryption Unit," *PKI*, 2016, http://www.pki-electronic.com/products/interception-and-monitoring-systems/active-gsm-monitoring-system-with-imsi-catcher-and-decryption-unit/.
11. "Cellular Interception," *Ability*, http://www.interceptors.com/intercept-solutions/Cellular-Interception.html.
12. "Ability IBIS Airborn [*sic*] movie," *YouTube*, uploaded by Anatoly Hurgin, Aug. 27, 2015, https://www.youtube.com/watch?v=Iep8Ix81ltA&feature=youtu.be.
13. Ibid.
14. Tim Cushing, "Israeli made Stingray Device Found in the Hands of South African Businessmen," *techdirt*, Aug. 14, 2015, https://www.techdirt.com/articles/20150811/10003831913/israeli-made-stingray-device-found-hands-south-african-businessmen.shtml; http://www.arrowcell.com/arrowcell_productpage.pdf.
15. 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/. Also see "Stingray," *Trademarkia*, http://www.trademarkia.com/stingray-76303503.html.

16. Bruce Schneier, "The Further Democratization of Stingray," *Schneier on Security*, Apr. 27, 2015, https://www.schneier.com/blog/archives/2015/04/the_further_dem_1.html.
17. "Government Cell Phone Surveillance Catalogue," *The Intercept*, Dec. 17, 2015, https://theintercept.com/document/2015/12/16/government-cellphone-surveillance-catalogue/.
18. "VME – Cell Phone Interceptors," *Meganet Corporation*, 2011, http://www.meganet.com/meganet-products-cellphoneinterceptors.html.
19. "3G-GSM Tactical Interception & Target Location," *Gamma Group*, n.d., https://info.publicintelligence.net/Gamma-GSM.pdf.
20. "IMSI catcher," *Alibaba*, http://www.alibaba.com/product-detail/IMSI-catcher_135958750.html; http://www.alibaba.com/product-detail/automatically-catcher-IMEI-IMSI-Mobile-phone_60291064962.html?spm=a2700.7724857.29.345.lqtFAs; http://www.alibaba.com/product-detail/ejoin-promotion-goip-32-channels-gateway_60423271279.html?spm=a2700.7724857.29.82.lqtFAs
21. Jeremy Scahill and Margot Williams, "Stingrays: A Secret Catalogue of Government Gear for Spying on Your Cellphone," *The Intercept*, Dec. 17, 2015, https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/.
22. Nathan Wessler, "CELLBRITE Data Recovery/SSE," *The Intercept*, Dec. 17, 2015, https://theintercept.com/surveillance-catalogue/cellbrite/.
23. "Government Cell Phone Surveillance Catalogue." Another document of interest is a 2011 catalogue from UK company Eskan. It is archived in Wikileaks' SpyFiles, which is available here: https://wikileaks.org/spyfiles/docs/ESKAN_2011_ElecSurvCoun_en.html.
24. See Chris Paget's presentation here: "Defcon 18 - Practical Cellphone Spying - Chris Paget - Part.mov," *YouTube*, uploaded by Hacking Conferences, Information Security, how to's, Dec. 12, 2010, https://www.youtube.com/watch?v=DU8hg4FTm0g.
25. Eugen Kabelmast, "DIY Quick & Dirty IMSI Catcher (and Snowden/Russian Psychology)," *KABELMAST*, July 25, 2013, https://kabelmast.wordpress.com/2013/07/25/diy-quick-dirty-imsi-catcher-and-snowdenrussian-psychology/.

26. Dan Goodin, "Low-cost IMSI catcher for 4G/LTE networks tracks phones' precise locations, *ars technica*, Oct. 28, 2015, http://arstechnica.com/security/2015/10/low-cost-imsi-catcher-for-4glte-networks-track-phones-precise-locations/.
27. Schneier
28. Stephanie Pell and Christopher Soghoian, "Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy," Dec. 29, 2014, *Harvard Journal of Law and Technology* 28, no. 1 (2014): 1-75.
29. Andreas Bakke Foss, Per Anders Johansen, and Fredrik Hager-Thoresen, "Secret surveillance of Norway's leaders detected," *Aftenposten*, Dec. 16, 2014, http://www.aftenposten.no/nyheter/iriks/Secret-surveillance- of-Norways-leaders-detected-7825278.html; Tyler Lopez, "How Did Ukraine's Government Text Threats to Kiev's EuroMaidan Protesters?" *Slate*, Jan. 24, 2014, http://www.slate.com/blogs/future_tense/2014/01/24/ukraine_texting_euromaidan_protesters_kiev_demonstrators_receive_threats.html; Tim Cushing, "Israeli-Made Stingray Device Found In The Hands Of South African Businessmen," *techdirt*, Aug. 14, 2015, https://www.techdirt.com/articles/20150811/10003831913/israeli-made-stingray-device-found-hands-south-african-businessmen.shtml.
30. "EPIC v. FBI – Stingray / Cell Site Simulator," *Electronic Privacy Information Center*, 2016, http://epic.org/foia/fbi/stingray/.
31. For more information on *United States v. Rigmaiden*, see the court decision at http://www.leagle.com/decision/In%20FDCO%2020130508G77/U.S.%20v.%20RIGMAIDEN#. For more information on Judge Brian Owsley's 2012 decision in the Texas case, see the court document "In the Matter of an Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device," at https://www.documentcloud.org/documents/479404-txopinion1.html#document/p1.
32. Hanna Fakhoury, "Stingrays Go Mainstream: 2014 in Review," *Electronic Frontier Foundation*, Jan. 2, 2015, https://www.eff.org/deeplinks/2015/01/2014-review-stingrays-go-mainstream.

33. Hanna Fakhoury and Trevor Timm, "Stingrays: The Biggest Technology Threat to Cell Phone Privacy You Don't Know About," *Electronic Frontier Foundation*, Oct. 22, 2012, https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy.
34. EPIC's FOIA request can be found at http://epic.org/foia/fbi/stingray/EPIC-FOIA-Request.pdf. For further information about the first phases of responses to the request, see Jason Koebler, "FBI Releases "Cell Phone Tracking for Dummies," Plus 4,999 [Redacted] Documents," *MOTHERBOARD*, Apr. 30, 2015, http://motherboard.vice.com/read/fbi-releases-cell-phone-tracking-for-dummies-plus-4999-redacted-documents.
35. Many of the documents are marked declassified FOUO or sensitive but unclassified or "secret," which is crossed out. Some of them indicate legal shifts after the Patriot Act and the extension of "trap and trace" methods that use cell phones. One set of slides in the fifth release shows the impact of the Patriot Act by including the laws both before and after the Act's passage.
36. Val Van Brocklin, "A brief review of 14 court cases on cell phone search incident to arrest," *PoliceOne.com*, Aug. 21, 2013, https://www.policeone.com/investigations/articles/6398708-A-brief-review-of-14-court-cases-on-cell-phone-search-incident-to-arrest/.
37. Sam Richards, Jason Hernandez, and Jerod MacDonald-Envoy, "[UPDATE-2] Cellphone Surveillance Used on Black Lives Matter Protesters in Fourth Precinct Minneapolis," *North Star Post*, Dec. 7, 2015, http://nstarpost.com/17486/159855/a/cellphone-surveillance-used-on-black-lives-matter-protesters-at-fourth-precinct; Mike Krauser, "Activists Say Chicago Police Used 'Stingray' Eavesdropping Technology During Protests," *CBS Chicago*, Dec. 6, 2014, http://chicago.cbslocal.com/2014/12/06/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/.
38. Anonymous, "Stingray Warrantless Wiretap by CPD on Activists, *YouTube*, uploaded by anon2world, Dec. 5, 2014, https://www.youtube.com/watch?v=xpdpjX8Vsfw; also see Brandon Smith, Paul Gottinger, et al., "Anonymous: Chicago Police Surveilled Activists, Including Politician's Daughter," *Reader Supported News*, Dec. 7, 2014, http://readersupportednews.org/news-section2/318-

66/27362-focus-anonymous-chicago-police-surveilled-activists-including-politicians-daughter.

39. Justin Fenton, "Baltimore Police used secret technology to track cellphones in thousands of cases," *Baltimore Sun*, Apr. 9, 2015, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-case-20150408-story.html.
40. See a draft of the bill here: https://chaffetz.house.gov/sites/chaffetz.house.gov/files/Cell%20Site%20Simulator%20Bill.pdf
41. Sanjay Singh, "Government hunts for elusive bug: DoT wants snooping and listening devices within private sector surrendered," *Daily Mail India*, 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#ixzz3uKkduw12.
42. Mary-Ann Russon, "China Arrests 1,500 People for Sending Spam Text Messages from Fake Mobile Base Stations," *International Business Times*, Mar. 27, 2014, http://www.ibtimes.co.uk/china-arrests-1500-people-sending-spam-text-messages-fake-mobile-base-stations-1442099.
43. Pierluigi Paganini, "China spies on airline passengers with IMSI-catchers," *security affairs*, Sept. 23, 2015, http://securityaffairs.co/wordpress/40380/cyber-crime/airline-passengers-imsi-catchers.html.
44. Schneier.
45. Kenneth Page, "Swiss Government forced to reveal destinations, cost of surveillance exports," *Privacy International* website, Jan. 14, 2015, https://www.privacyinternational.org/node/98.
46. "Stingray Tracking Devices: Who's Got Them?," *American Civil Liberties Union*, 2015, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them/.
47. "Android IMSI-Catcher Detector," *HACKADAY.IO*, https://hackaday.io/project/3824-android-imsi-catcher-detector; SecUpwN, "Android IMSI-Catcher Detector," *Github*, https://secupwn.github.io/Android-IMSI-Catcher-Detector/.
48. Andrew Rosenblum, "Mysterious Phony Cell Towers Could be Intercepting Your Calls," *Popular Science*, Aug. 27, 2014, http://www.popsci.com/article/technology/mysterious-phony-cell-towers-could-be-intercepting-your-calls; EDS America, Cryptophone

promotion, https://esdcryptophone.com/download/ESD-Cryptophone-CP500i.pdf.

49. Adrian Dabrowski, Nicola Pianta, et al., "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," *ACSAC 14*, Dec. 8-14, https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf; Kade Crockford et al., "Spidey: Android-based Stingray Detector," *Github*, 2014, http://jtwarren.github.io/files/spidey.pdf
50. Anthony Giddens, *The Nation-State and Violence* (Berkeley and Los Angeles: University of California Press, 1987), 294-335.
51. "Phone Hackers: Britain's Secret Surveillance," *YouTube*, uploaded by Vice News, Jan. 14, 2016, https://www.youtube.com/watch?v=rzBWoVh4qhk.
52. For more on "infrastructural disposition," see Lisa Parks, "'Stuff You Can Kick': Toward a Theory of Media Infrastructures" in *Between Humanities and the Digital*, Patrik Svensson and David Theo Goldberg, eds. (Cambridge, MA: MIT Press, 2015), 355–373.
53. 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.

Lisa Parks is Professor and former Department Chair of Film and Media Studies (2008-2011) and served as Director of the Center for Information Technology and Society (CITS) at UC Santa Barbara from 2012-2015. Parks has research expertise in the areas of media history and theory, media and globalization, media arts and activism, digital cultures, experimental methodologies, and feminist criticism. She has written extensively about satellites as cultural technologies, and her current research is focused in two related areas: media infrastructure studies; and media, security and surveillance studies. Parks is the author of *Cultures in Orbit: Satellites and the Televisual* (Duke UP, 2005), *Coverage: Vertical Mediation and the War on Terror* (Routledge, forthcoming), and *Mixed Signals: Media Infrastructures and Cultural Geographies* (in progress). She is co-editor of*: Signal Traffic: Critical Studies of Media Infrastructures* (U of Illinois, 2015), *Down to Earth: Satellite Technologies, Industries and Cultures* (Rutgers UP, 2012), Undead TV (Duke UP, 2007) *Planet TV: A Global Television Reader* (NYU, 2003), and another in progress entitled *Life in the Age of Drones* (under contract, Duke UP).