Wiretapping Stuff: Notes on Sound, Sense, and Technical Infrastructure
Author(s): Brian Hochman
Source: *Resilience: A Journal of the Environmental Humanities*, Vol. 5, No. 3, Common Senses and Critical Sensibilities (Fall 2018), pp. 96-108
Published by: University of Nebraska Press
Stable URL: https://www.jstor.org/stable/10.5250/resilience.5.3.0096
Accessed: 10-09-2018 19:32 UTC

Wiretapping Stuff

Notes on Sound, Sense, and Technical Infrastructure

BRIAN HOCHMAN

This article reconsiders key concepts in the field of sound studies in light of new theories of media materialism. My focus is on the relationship between electronic eavesdropping and technical infrastructure, a foundational area of modern media culture that has long proved difficult to assimilate into received models of inquiry. Before launching into my analysis, I want to offer two brief stories as points of departure.

***

Story number one is about a rogue stock broker named D. C. Williams, who was at one time the most notorious professional eavesdropper in the United States. Williams made his name by tapping into the electronic communications of several prominent business entities based in California, intercepting secrets about board decisions and financial performance. He then relayed that information to a group of paying subscribers, who in turn made financial moves based on the intelligence that Williams had gathered. The genius of the scheme wasn't just that it allowed Williams to eavesdrop on confidential conversations. It also capitalized on the time it takes to send an electronic message across a region as vast as that of the continental United States (a short period of time but a period of time nonetheless). Using highly sophisticated techniques, Williams found a way to communicate inside information with his syndicate while slowing the speed with which the original corporate messages reached their intended destinations. His subscribers

could buy and sell stocks before anyone else on the East Coast, taking advantage of illegal tips while appearing to go along with the daily fluctuations of the market.

The scheme proved lucrative. Williams's correspondence, later confiscated by authorities, revealed that the members of his syndicate had made a small fortune in the short time the wiretapping conspiracy was up and running. But the setup proved too good to be true. Acting on inside information of their own, authorities nabbed Williams in the act of tapping the corporate network. He was soon prosecuted and convicted under an obscure California statute prohibiting the interception of electronic messages. Reporters covering the story deemed it a "new chapter in crime," a reminder that eavesdropping was an inevitable byproduct of the age of electronic communications.[1]

The year—and here's the twist to the story—was 1864.

***

Story number two takes place almost 150 years later. In June 2013 Edward Snowden, former National Security Administration (NSA) contractor turned whistleblower, revealed that the US government was monitoring the world's digital communications by tapping into a vast network of undersea cables that spanned the globe. The program was called Upstream, and the name—by turns a technical designation for a type of electronic eavesdropping and a handle for a suite of clandestine NSA programs that employ it widely—soon became synonymous with warrantless government surveillance in the United States. On the heels of widespread outrage over PRISM, a massive data-sharing program between the NSA and nine major US Internet companies, revelations about Upstream gave many Americans the impression that no trace of digital data was beyond the state's reach.

Upstream wasn't an unprecedented government surveillance program. The NSA had been regularly tapping undersea telecommunications networks since the early 1970s. But in order to understand the type of surveillance the NSA was doing in 2013, you needed to know something about how we communicate digitally, a tall order for those of us who take the technical workings of the Internet for granted. News coverage of the Upstream revelations typically resorted to a stock set of figures to help the average US citizen grasp

what was at stake. We were told that 550,000 miles of undersea fiber-optic cable connects the world's Internet users. Upward of 99 percent of transcontinental Internet traffic travels through those cables on any given day. By tapping into the undersea network at strategic choke points—physical sites at which fiber-optic cables either intersect or surface on land—the federal government could monitor vast amounts of digital data.[2]

The name of the Upstream program contained hints about the technical processes that enabled its use. If communicating in the digital age can be likened to sending a bundle of messages down an invisible river of bits and bytes, the NSA seemed to have the ability to snatch the contents of those messages "upstream," before they reached their destination. But in those early days Upstream was perhaps best understood in visual terms, and it is most often remembered as such today. The earliest public reports on the program, first published in the *Washington Post* and the *Guardian*, usually included a low-resolution screenshot taken from one of the top-secret NSA slides that Snowden had leaked to the press.[3] In it, below an inserted explanation of Upstream ("collection of communications on fiber cables . . . as data flows past") and above an explanation of PRISM ("collection directly from the servers of . . . U.S. [Internet] Service Providers"), was a map of North America, with brownish-maroon lines spilling out into the Atlantic and Pacific Oceans. Yellow and blue circles crudely indicated where the NSA was in the process of monitoring the world's digital traffic. Notably, the content of our data, flowing swiftly down the river of communications, wasn't pictured in the image. What mattered was the river itself—the brownish-maroon lines radiating out from the continent, the vast network of fiber-optic cables snaking through the depths of the sea.

The image seemed to say, "Your personal information travels along these channels. We know where they are, and that's where we tap the wires."

***

I first encountered story number one while finishing my first book. The description of D. C. Williams's corporate wiretapping scheme was buried in the columns of a nineteenth-century newspaper. I probably

wouldn't have given the episode much thought if story number two, the story of Upstream, hadn't been making headlines around the same time. Reading the two stories together induced an eerie sort of historical vertigo. Williams was eavesdropping on telegraph messages, not telephone exchanges or digital communications. The obscure California statute under which he was eventually prosecuted was written in 1862, which means that wiretapping was common enough in the Golden State for lawmakers to enact a prohibition against the practice during the Civil War. Obviously we shouldn't regard Williams's wiretapping syndicate as an ancestral precursor to Upstream. There's too much variation in technology, scale, and intent for that sort of thinking. But the superficial similarities between the two stories make one thing certain: today's debates about communications privacy are merely the most recent chapter of a much longer history. Wiretapping and electronic eavesdropping are actually as old as electronic communications themselves.

Taken together, the stories of D. C. Williams and Upstream offer us two important lessons about electronic eavesdropping—lessons that expose, more generally, the limitations of using the senses (visual, aural, etc.) as heuristic guides for the study of media history. The first lesson is that eavesdropping in the electronic age isn't exclusively, or even primarily, an act of listening. This is an argument that contradicts a received consensus in the extant body of scholarly work on electronic surveillance. According to the French philosopher Peter Szendy, whose recent book on the subject has already emerged as a touchstone in the field of sound studies, "Listening and espionage [are] inextricably implicated [in] each other in their respective histories." Drawing on a wide range of cultural and philosophical texts, Szendy goes on to posit that the relationship between sound and surveillance is so close that "every listener is . . . above all a spy."[4] But do cases like that of D. C. Williams actually fit in with these sorts of transhistorical claims? To be sure, the corporate spy Williams was an adept listener. The first step of the 1864 conspiracy apparently involved getting within earshot of a telegraph sounder to decipher the contents of each corporate transmittal. "Williams is an expert at telegraphing and reads 'by sound,'" the original article on his criminal exploits reported. "Taking the messages as they passed . . . he could sit within hearing of the instrument and make himself familiar with all that transpired."[5] But the success of Williams's scheme—and its importance to the history

of electronic eavesdropping in the United States, as we'll soon see—hinged on interactions with technology that fall outside the realm of the auditory: cutting into wires and destroying copies of messages, trespassing on secure areas to gain proximity to relevant equipment, and even bribing telegraph company employees to help delay corporate messages from reaching their intended recipients.[6] The diversity of these activities should remind us, contra Szendy, that eavesdropping isn't always an affair of the ears. Government surveillance programs like Upstream operate in a similar gray area in terms of their relationship to the senses. Only a small portion of what the NSA does today can actually be characterized as listening. Based on the documents that Snowden leaked in 2013, we know that Upstream "harvests," "intercepts," "collects," "stores," "filters," and "mines." But to say that the NSA *overhears* our digital communications is more often than not to employ an anachronism, a fact that Szendy himself fleetingly admits in the preface to a new English-language translation of his book.[7]

Approaching the history of wiretapping and electronic eavesdropping solely from the perspective of the once-nascent but now quite durable field known as sound studies may therefore obscure as much as it reveals. My primary contention here is that what is obscured, above all else, is electronic eavesdropping's dependence on the existence and integrity of *media infrastructures*—its dependence on the material systems through which cultural information is trafficked in our networked society. This is the second lesson of the D. C. Williams and Upstream stories. By now scholars have written a great deal about the centrality of sound and sound technologies to modernity.[8] But we haven't done enough to consider the infrastructures that enable (and disable, as the case may be) the social phenomena that interest thinkers like Szendy. From the telegraph wires in the story of D. C. Williams to the undersea cables in the story of Upstream, the history of wiretapping and electronic eavesdropping in the United States brings this fundamental reality of our mediascape into view. If we truly want to understand the workings of sound in the modern era, don't we first need to understand the technical systems—the infrastructures—through which sound itself travels? Or to ask the question in a somewhat different manner: Is it possible to speak of wiretapping without also speaking of the wires?

***

My thinking here builds on the work of Lisa Parks, Nicole Starosielski, and a host of like-minded scholars and artists who have recently drawn attention to the material infrastructures on which our seemingly immaterial media culture has always depended: technical equipment, natural resources, laboring bodies—"stuff you can kick," as Parks puts it.[9] Infrastructural technologies like roads and sewer systems have long been regarded as hallmarks of modernity. According to Paul N. Edwards, "to be modern is to live within and by means of infrastructures."[10] But only recently have scholars come to see infrastructures as the "underbelly of modern media."[11] The workings of our global culture of sound, image, and communicative data flow are typically imagined as virtual and automated, in the air and without a trace. Yet without the physical hardware that forms the backbone of the Internet—established in real environments, maintained by actual people, embedded in the fabric of social life—our virtual and automated world wouldn't exist.[12]

The long-standing cliché in the study of infrastructures is that they are at once imperceptible (because they are too vast for us to imagine them in their totality) and invisible (because we don't think about them until they break down or become obsolete).[13] But Parks argues that when we approach infrastructures "dispositionally," inferring their existence beyond the immediate points at which they make themselves known, we're able to understand where they are, how they work, and why they matter.[14] This has two important consequences for the study of audiovisual media. On one hand, it allows us to follow the formal channels through which cultural information flows rather than simply interpret, on the level of content, what it represents and how we receive it. As Parks and Starosielski argue in a recent volume on the subject, paying close attention to infrastructure "foregrounds *processes of distribution* that have taken a backseat in humanities-based research on media culture, which until recently has tended to prioritize processes of production and consumption, encoding and decoding, and textual interpretation."[15]

On the other hand, any attempt to understand technical infrastructure necessarily entails conceiving of media history outside critical models that have remained dominant since Marshall McLuhan first identified media technologies as "extensions" of the human sensorium in the early 1960s.[16] Technical infrastructures, Parks and Starosielski continue, ultimately reveal the "unique *materialities* of

media distribution—the resources, technologies, labor, and relations that are required to shape, energize, and sustain the distribution of audiovisual signal traffic on global, national, and local scales."[17] If we begin to think infrastructurally, sounds and images, hearing and vision, begin to matter less in the history of audiovisual media. The senses matter less. What matters is a broader media ecology, supported and shaped by technical infrastructure.

My own argument is that wiretapping and electronic eavesdropping are products of media infrastructure. They are constitutive of the material systems that make up our communications networks, and over time they have made the hidden hardware and labor behind our modern media culture both visible and perceptible. This was as true 150 years ago as it is today. The D. C. Williams case, for example, raised vexing questions about the physical channels through which electrical signals traveled from one side of the country to the other. How was it possible for Williams to have intercepted messages sent by wire? And how could he have waylaid those signals long enough to communicate their contents with the members of his syndicate and then released them to their intended recipients without anyone the wiser? Answering these questions required extensive consideration of telegraphic infrastructure. It required a language for understanding the channels and environments through which messages flowed, rather than the form or content of the messages themselves.

More tellingly, Williams was eventually prosecuted under a California state law that wasn't solely designed to ensure the privacy of telegraph messages. It was also intended to protect what lawmakers called the "fidelity" of the telegraph system (i.e., the integrity of its technical infrastructure).[18] Chapter 262, section 8, of the California statutes for 1862 states the following:

> If any person shall wilfully [*sic*] and maliciously cut, break, or throw down, any telegraph pole, or any tree, or other object, used in any line of telegraph, or shall wilfully and maliciously break, displace, or injure, any insulator in use in any telegraph line, or shall wilfully and maliciously cut, break, or remove from its insulators, any wire used as a telegraph line, or shall, by the attachment of a ground wire, or by any other contrivance, wilfully and maliciously destroy the insulation of such telegraph line, or

> interrupt the transmission of the electric current through the same, or shall in any other manner wilfully and maliciously injure, molest, or destroy, any property, or materials, appertaining to any telegraph line, or belonging to any telegraph company, or shall wilfully and maliciously interfere with the use of any telegraph line, or obstruct or postpone the transmission of any message over the same, or procure, or advise, any such injury, interference, or obstruction, the person so offending shall be deemed guilty of a misdemeanor, and shall be punished by fine, not to exceed five hundred dollars, or imprisonment, not to exceed six months, or by both such fine and imprisonment, in the discretion of the Court; and shall, moreover, be liable to the telegraph company whose property is injured or line obstructed, in a sum equal to one hundred times the amount of actual damages sustained thereby.[19]

In other words, tampering with the hardware that enabled telegraphic communications ("malicious injury to the telegraph," in the language of the law in 1862) was just as serious a matter as violating the privacy of telegraph messages themselves.[20] The two crimes went hand in hand. The first California Penal Code, written a decade later, went into more detail about protecting telegraph equipment and facilities, going so far as to include language about the bribing of telegraph officials.[21]

The language about "malicious injury" to telegraphic infrastructure in California's original wiretapping statute would fall out of the 1905 statute that extended the state's electronic communications laws to the telephone system. That statute simply reads,

> Every person who, by means of any machine, instrument, or contrivance, or in any other manner, willfully and fraudulently reads, or attempts to read, any message, or to learn the contents thereof, whilst the same is being sent over any telegraph or telephone line, or willfully and fraudulently, or clandestinely, learns or attempts to learn the contents or meaning of any message, while the same is in any telegraph or telephone office, or is being received thereat or sent therefrom, or who uses or attempts to use, or communicates to others, any information so obtained, is punishable as provided in section six hundred and thirty-nine.[22]

But the goal of protecting the physical hardware of the telephone

system—wires, terminal switches, junction boxes, and the like—was implicit in California's attempts to revise its eavesdropping regulations in accordance with the twentieth century's technological advancements. When the state amended the same statute in 1915, for instance, it reintroduced the "malicious injury" idea under the guise of preventing "unauthorized connection with any telegraph or telephone wire, line, cable, or instrument under the control of any telegraph or telephone company."[23] In the state of California, attempts to protect privacy and prohibit eavesdropping were thus indistinguishable from efforts to protect the security and integrity of the technical infrastructure.

More than a century later, infrastructure plays a central role in the ongoing controversies over electronic surveillance at the NSA, which have brought renewed attention to the physical systems and environments through which our data flows. As we've already seen, after decades of resting invisibly on the ocean floor, the network of fiber-optic cables that forms the backbone of the NSA's Upstream program became a point of public concern when the Snowden leak occurred in the summer of 2013. The Internet's hidden material infrastructure has even come to inspire artistic responses. The multimedia artist Trevor Paglen has recently undertaken a project to photograph underwater fiber-optic cables that the NSA and other international surveillance agencies are currently in the process of tapping. In *Bahamas Internet Cable System (BICS-1) NSA/GCHQ-Tapped Undersea Cable Atlantic Ocean* (2015) a coral-encrusted cable emerges from a muddy seafloor and recedes into a murky blue-green distance. In *Mid-Atlantic Crossing (MAC) NSA/GCHQ-Tapped Undersea Cable Atlantic Ocean (2015)* (2015), a cable no thicker than a garden hose peaks out from a wide plain of sand only to disappear in the middle of the frame, as if buried by the movement of currents and the passage of time. Such images force us to confront the fact that the geography of state surveillance is part of the geography of the natural world and vice versa. For Paglen, digital-surveillance infrastructure is at once embedded in oceanic environments and obscured by it, a relationship that seems to typify the media theorist Jussi Parikka's idea of "medianatures": while "relations with the earth are mediated through technologies," the earth itself "provides for media and enables it."[24]

Paglen's underwater-cable photographs recall his more well-known practice of taking pictures of aerial surveillance drones with high-

powered telephoto lenses, the point of which, he told *The New Yorker* in 2012, wasn't "to expose and edify so much as to confound and unsettle." Trained at, and obscured by, surreal technicolor skies rather than murky underwater depths, Paglen's drone photographs, he continues, are "useless as evidence . . . but at the same time they're a way of organizing your attention."[25] One can't help but read Paglen's latest work as the natural extension of this artistic impulse. The underwater-cable series lays bare a digital-media infrastructure that's otherwise "submerged," both literally and figuratively. At a recent gallery show at Metro Pictures in New York, moreover, Paglen displayed photographs like *Bahamas Internet Cable System* and *Mid-Atlantic Crossing* alongside photographs of coastal locations where fiber-optic cables land and link up with aboveground communications terminals. He also provided detailed maps of tapped-cable choke points in the United States and Britain. Clearly, Paglen's interest is in providing aesthetic keys and real-world referents to the abstract NSA PowerPoint slide that showed the workings of Upstream to the world in 2013, and he provocatively describes the stakes of such an artistic revelation in terms that resonate with Lisa Parks's work on infrastructural imaginaries: "When we talk about the Internet or mass surveillance, we use horribly mystifying metaphors to describe them: the cloud, the world wide web, the Information Superhighway, and so on. . . . But everything in the world is made of *stuff*, right? Where is the stuff that . . . [electronic] surveillance is made of, and what does it look like?"[26]

Paglen's photographs ultimately draw our attention to the "stuff"—the material infrastructure—that enables wiretapping and electronic eavesdropping in the digital age. But the question he asks can just as easily apply to the past buried beneath the veneer of the digital, and the answer is as applicable to the telegraph in the nineteenth century as it is to the Internet in the twenty-first. There is no such thing as wiretapping without wires. Eavesdropping is a constitutive product of infrastructure; it depends on stuff you can kick. We'd do well to give that stuff our attention.

Brian Hochman is an associate professor of English and a core faculty member of American studies and film and media studies at Georgetown University. He is the author of *Savage Preservation: The Ethnographic Origins of Modern Media Technology* (Minneapolis: University of Minnesota Press, 2014), which was named as a finalist for the American Studies Association's Lora Romero

Prize for Best First Book in 2015. His current book, *The Uninvited Ear: A History of Wiretapping in the United States*, is forthcoming from Harvard University Press and funded by a 2017–18 National Endowment for the Humanities Public Scholar Fellowship.

NOTES

1. "Tapping the Wires for Stock Operations," *Sacramento Daily Union*, August 12, 1864.

2. See Craig Timberg and Ellen Nakashima, "Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance," *Washington Post*, July 6, 2013, https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html?utm_term=.7efab0965d20; Olga Khazan, "The Creepy, Long-Standing Practice of Undersea Cable Tapping," *Atlantic*, July 16, 2013, http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/. For an overview of the PRISM and Upstream programs, see David P. Fidler, "NSA PRISM and UPSTREAM Briefing Slides," in *The Snowden Reader*, ed. David P. Fidler (Bloomington: University of Indiana Press, 2015), 96–100.

3. See "NSA Slides Explain the PRISM Data-Collection Program," *Washington Post*, last updated July 10, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/; James Ball, "NSA's PRISM Surveillance Program: How It Works and What It Can Do," *Guardian*, June 8, 2013, http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google.

4. Peter Szendy, *All Ears: The Aesthetics of Espionage*, trans. Roland Végsö (New York: Fordham University Press, 2017), 9, 6.

5. "Tapping the Wires for Stock Operations."

6. "Tapping the Wires for Stock Operations."

7. Szendy, *All Ears*, x.

8. A complete bibliography of scholarship in this still-growing area is impossible to compile for the purposes of this article. Notable titles, however, include R. Murray Schafer, *The Soundscape: Our Sonic Environment and the Tuning of the World* (1977; repr., Rochester, VT: Destiny Books, 1994); Friedrich Kittler, *Gramophone, Film, Typewriter*, trans. Geoffrey Winthrop-Young and Michael Wutz (1986; repr., Stanford, CA: Stanford University Press, 1999), 21–114; James Lastra, *Sound Technology and the American Cinema: Perception, Representation, Modernity* (New York: Columbia University Press, 2000); Jonathan Sterne, *The Audible Past: Cultural Origins of Sound Reproduction* (Durham, NC: Duke University Press, 2003); Peter Szendy, *Listen: A History of Our Ears*, trans. Charlotte Mandell (New York: Fordham University Press, 2008); Jonathan Sterne, *MP3: The Meaning of a Format* (Durham, NC: Duke University Press, 2012); selected entries in *Keywords in Sound*, ed. David Novak and Matt Sakakeeny (Durham, NC: Duke University Press, 2015), 65–77, 99–111.

9. Lisa Parks, "'Stuff You Can Kick': Toward a Theory of Media Infrastructures," in *Humanities and the Digital*, ed. David Theo Goldberg and Patrik Svensson (Cambridge, MA: MIT Press, 2015), 355. See also, among others, Lisa Parks, "Around the Antenna Tree: The Politics of Infrastructural Visibility," *Flow*, March 2009; Lisa Parks, "Media Infrastructures

and Affect," *Flow*, May 2014; Nicole Starosielski, *The Undersea Network* (Durham, NC: Duke University Press, 2015); John Durham Peters, *The Marvelous Clouds: Toward a Philosophy of Elemental Media* (Chicago: University of Chicago Press, 2015), 30–38; the essays collected in *Signal Traffic: Critical Studies of Media Infrastructures*, ed. Lisa Parks and Nicole Starosielski (Urbana: University of Illinois Press, 2015).

10. Paul N. Edwards, "Infrastructure and Modernity: Force, Time, and Social Organizations in the History of Sociotechnical Systems," in *Modernity and Technology*, ed. Thomas J. Misa, Philip Brey, and Andrew Feenberg (Cambridge, MA: MIT Press, 2003), 186. Edwards goes on to argue that infrastructures are so central to the workings of the modern that they can only be understood in negative terms: "Given the heterogeneous character of systems and institutions referenced by the term, perhaps 'infrastructure' is best defined . . . as those systems without which contemporary societies cannot function" (187).

11. Parks, "'Stuff You Can Kick,'" 364. Christian Sandvig's "The Internet as Infrastructure," in *The Oxford Handbook of Internet Studies*, ed. William H. Dutton (New York: Oxford University Press, 2013), 86–106, provides a fine overview of the move toward infrastructure in the study of media history. See also Brian Larkin, "The Politics and Poetics of Infrastructure," *Annual Review of Anthropology* 42, no. 1 (2013): 327–43.

12. On the "physicality of the virtual," see Paul Dourish and Genevieve Bell, "The Infrastructure of Experience and the Experience of Infrastructure: Meaning and Structure in Everyday Encounters with Space," *Environment and Planning B* 34, no. 3 (2007): 424.

13. See Susan Leigh Star, "The Ethnography of Infrastructure," *American Behavioral Scientist* 43, no. 3 (1999): 381–82.

14. Parks, "'Stuff You Can Kick,'" 357, 359.

15. Parks and Starosielski, *Signal Traffic*, 5; emphasis in original.

16. Marshall McLuhan, *Understanding Media: The Extensions of Man* (1964; repr., Cambridge, MA: MIT Press, 1994).

17. Parks and Starosielski, *Signal Traffic*, 5; emphasis in original. On media and materiality, see Jussi Parikka, *What Is Media Archaeology?* (Cambridge, UK: Polity Press, 2012), 63–89; Jussi Parikka, *A Geology of Media* (Minneapolis: University of Minnesota Press, 2015).

18. Cal. Stat., chap. 262, § 1–19 (1862). For more on the early history of eavesdropping law in the state of California, see H. Lee Van Boven, "Electronic Surveillance in California: A Study in State Legislative Control," *California Law Review* 57, no. 5 (November 1969): 1182–1256.

19. Cal. Stat., chap. 262, § 8 (1862).

20. Cal. Stat., chap. 262, § 8 (1862).

21. Cal. Pen. Code § 640 (1872).

22. Cal. Stat., chap. 528, § 6 (1905).

23. Cal. Stat., chap. 117, § 1 (1915).

24. Parikka, *Geology of Media*, 12–13.

25. Jonah Weiner, "Prying Eyes: Trevor Paglen Makes Art out of Government Secrets," *New Yorker*, October 22, 2012, http://www.newyorker.com/magazine/2012/10/22/prying-eyes. On Paglen's work on drones and other technologies of the modern surveillance state, see Thomas Keenan, "Disappearances: The Photographs of Trevor Paglen," *Aperture* 191

(Summer 2008), 36–43; Julian Stallabrass, "Negative Dialectics in the Google Era: A Conversation with Trevor Paglen," *October* 138 (Fall 2011), 3–14.

26. Zach Sokol, "Trevor Paglen Photographs the Underwater Telecommunication Cables Tapped by the NSA," *Vice*, September 9, 2015, http://www.vice.com/read/the-map-is-the-territory-0000742-v22n9; emphasis in original.