Surveillance from the Middle
On Interception, Infrastructure, and the Material Flows of Asynchronous Communication

Jason Farman

In August 2014, *Popular Science* published a story that quickly spread to other news venues and online sites. Titled "Mysterious Phony Cell Towers Could be Intercepting Your Calls," the report detailed the discovery of at least seventeen interceptor cell towers in the United States that tricked mobile devices into believing they were connecting to their carriers' cell antennas.[1] Each intercepted phone was instead connecting to a dummy tower that, after collecting information from the phone, passed it over to the "real" tower. The story developed for several weeks, as more and more of these interceptor towers were discovered by "ultra-secure" mobile phones that could identify these pseudo-towers' attempts to intercept the cell signals.

Members of the public began to formulate theories about who was setting up these interceptor towers and what their motives were. Newspapers and online news sites ran stories with headlines such as, "Are the mysterious "interceptor" cell towers the handiwork of foreign entities?"[2] Comments in these reports exploded with speculation about who set up these interceptor towers, from terrorist organizations and domestic drug cartels to the National Security Agency and the very corporation who identified the

mystery towers with its ultra-secure mobile phones. It seemed like everyone wanted to know who was surveilling their mobile phone usage and why.

The mystery of these interceptor towers was actually solved three years *prior* to the story being published in *Popular Science*. Daniel Rigmaiden, serving time in prison for filing fraudulent tax returns, discovered that the Federal Bureau of Investigation had found him through one of these interceptor towers. Yet, these were not cell towers at all. Instead, Rigmaiden uncovered that a device called a StingRay, which sent signals into neighborhoods in an attempt to locate a particular mobile device, had located him.[3] The StingRay is a cell site simulator, or an IMSI catcher (IMSI stands for "international mobile subscriber identity," a unique identificatory code for cellphones), that sends out pings to all phones within the vicinity of the device.[4] All phones in the area ping back, as if the mobile devices were sending information back to their carrier's nearest cell tower (which is used to keep a phone in constant contact with the carrier's network). Eventually, the StingRay identifies the phone that is being sought, usually under the operation of local law enforcement. So, while the cell site simulator is hunting for a particular phone (or set of phones, as utilized in the President's motorcade to "protect him from attacks and alert the Secret Service to people who shouldn't be near the President"[5]), one side effect is that it gathers data from every phone within its reach.

The surveillance practices of the cell-site simulator bring up many important aspects about the ways surveillance is understood and theorized. First, the spatial metaphors for surveillance often obfuscate the dynamic arrangements under which surveillance is practiced. That is, terms like surveillance ("to watch from above"), sousveillance ("to watch from below"), or lateral/participatory surveillance ("non-hierarchical watching") all miss the ways that many surveillance practices operate "from the middle" or from a multi-sited position. Interception troubles the traditional spatial metaphors for surveillance. As such, the material realities of surveillance-via-interception are often unknown to those being watched. This article thus traces the relationship between these two things: the spatial arrangements of "surveillance from the middle" and the ways these arrangements veil the materialities of interception and surveillance.

Interception and Mediation

Surveillance from the middle can be understood as mediation in its most basic form. This gestures back to the term "medium" in the nineteenth-century sense of the word: "An intervening substance through which a force acts on objects at a distance or through which impressions are conveyed to the senses; any substance considered with regard to its properties as a vehicle of light or sound."[6] A medium's common associations with a message or the carrying of content would not surface until much later, perhaps finding its resonance as a "communication medium" against the backdrop of electricity in the 1880s. As Lisa Gitelman and Theresa M. Collins write, "Throughout the nineteenth century a medium was "an intervening agency or substance". So, for instance, United States patents that used the plural form, *media*, in the nineteenth century do so with greatest frequency in reference to "filtering media", substances which work to filter solutions from more to less cloudy."[7] Here, surveillance from the middle is quite literally a medium as an "intervening agency" that works to filter "from more to less cloudy."

This mode of surveillance works particularly well with communication technologies that function asynchronously. As people send messages back and forth to one another, there is a necessary time/space lag that affords the possibility of interception. Concerns about interception echo throughout the history of correspondence. For instance, some cultures have resisted asynchronous written communications under the belief that oral messages delivered by a messenger were more difficult to intercept and thus more reliable.[8] In part, the fears of interception in letter writing were addressed by the introduction of wax seals to close a letter and serve as a material symbol of both its author (i.e., royal seals were unique to each monarch) and the fact that the letter had not been opened since the author had sealed it shut. Should the wax seal be broken, the recipient would know that the message inside was compromised.[9]

Figure 1. A wax seal from the Instituto Superior Técnico in Lisbon, Portugal. © [Domiriel](#), used by permission under Creative Commons Attribution Non-Commercial License.

In our own mobile media culture, we have once again come to prioritize asynchronous communication. Since 2009, data transfer—through means such as email, texting, status updates, and photo sharing—has outpaced voice communication on mobile devices. Thus, the time lag and spatial transfer of these messages are embedded in our everyday communication practices, which affords the opportunity for interception and surveillance from the middle. Here, it is worth noting that interception of this kind is unique from eavesdropping or wiretapping. While those do constitute a similar form of interception, practices like eavesdropping are simultaneous to the exchange of information instead of functioning as a medium that collects the message *before* the message can be delivered. At first glance, this may not seem to be a significant distinction, since both function in similar ways as modes of surveillance typically hidden from the communicators. However, the spatial arrangement has a larger impact on the ways that surveillance practices—and resistance to those practices—are understood. This significance is most clearly articulated by linking the spatial configuration of surveillance from the middle with its materiality.

Material Infrastructures of Surveillance from the Middle

The material structures and infrastructures that afford surveillance from the middle shape how messages flow between people. The affordances and constraints of asynchronous channels of communication create modes of practice that, in part, determine the situation for how these media are produced, distributed, consumed, and responded to. As such, surveillance from the middle practices are media that respond to the specificities of the media they interact with. In other words, interception-as-surveillance mediates (as an intervening agent) according to the particularities of the medium it seeks to intercept. This medium-specific mediation is thus a continual negotiation between the strategies of the one who is surveilling, which modes of interception are possible for a specific medium, and the tactics of those sending the message who attempt to circumvent its interception.

One example I came across recently illustrates this constant negotiation between these actors in this model of surveillance. During World War I, Walter Boadway was a cadet aviator stationed in France and other parts of Europe. He wrote letters constantly to his wife, Betty, who lived in Pasadena, California. As Betty began receiving his letters shortly after he was deployed, there were strange holes in the paper. Sometimes, entire portions of a page were missing from his letters. After this happened several times, she wrote to him to let him know that words and paragraphs from his letters were being removed for some reason. Military censors were not blacking out these parts of the letters. Instead, the censors were using X-Acto knives to literally remove any word or phrase that would compromise classified information (see Figure 2).
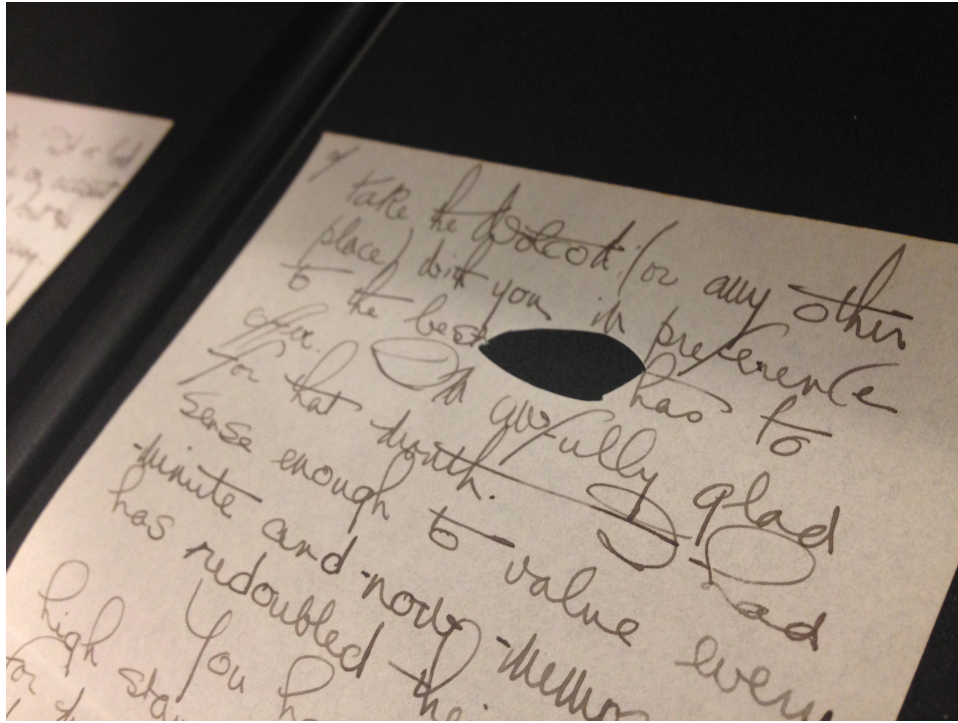
Figure 2. One of Walter Boadway's letters written during WWI, with a word removed by a military censor before the letter arrived to his wife in Pasadena, California. This letter is a part of the corpus of letters owned by the Center for American War Letters at Chapman University. Image © 2015 Jason Farman, reproduced by permission of the owner.

For Boadway, what constituted classified information remained mostly unknown, since those definitions were constantly changing in response to wartime circumstances. In his early letters to his wife, he had no sense that naming the kind of plane he flew was exposing information that would compromise the military's mission if it were intercepted. At one point, he was also told that he could not date his letters. Subsequently, instead of writing "November 11, 1917," he simply wrote "Sunday." Otherwise, the date would be cut out entirely by the military censors. As he wrote these early letters, he used both sides of a sheet of paper. After the military censors cut out the classified information, non-classified parts of the letters were rendered illegible as well (see Figure 3). Hence, the *material consequence* of writing something deemed classified was that the entire letter became more or less illegible due to the removal of pieces of the paper.
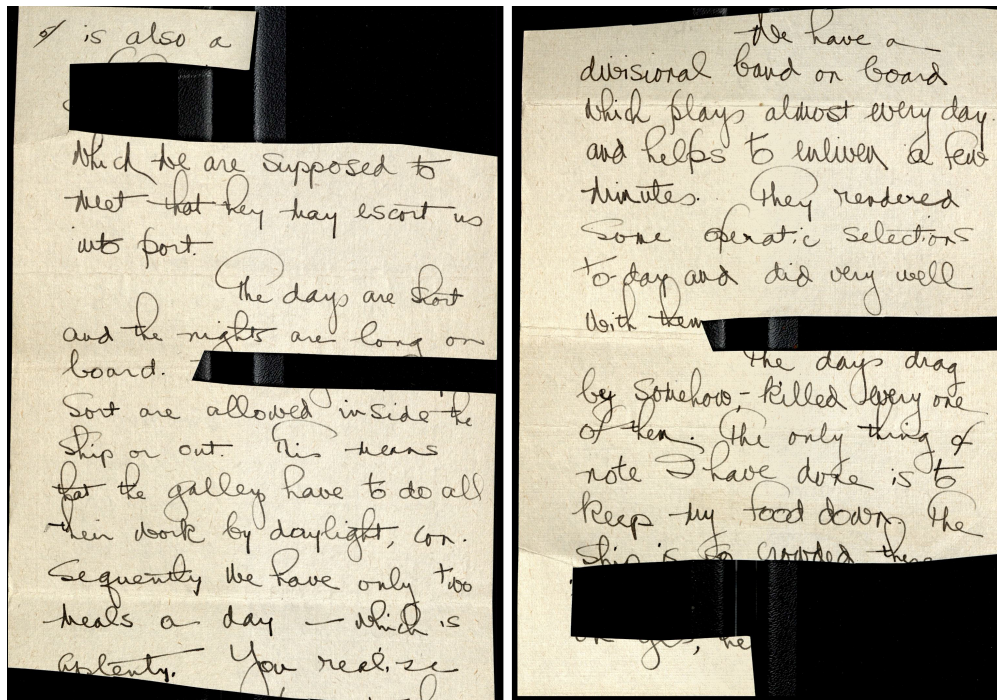
Figure 3. Two sides of the same censored sheet in one of Boadway's letters to his wife. This
letter is a part of the corpus of letters owned by the Center for American War Letters at
Chapman University. Image used by permission.

As these words, sentences, or paragraphs are brought under erasure through
the removal of the material piece of paper, words are removed but systems of
surveillance are revealed. Here, much in the way the broken wax seal on a
letter revealed that the letter had been read, the censor's cutting of the letter
revealed that interception was happening. For soldiers, inscribing words that
were prohibited resulted in the inability to communicate. But the removal of
the words in this way revealed the flow of communication to the people
attempting to correspond with each other: from author to censor to intended
recipient. (In some cases, the flow might instead run from author to censor to
enemy intelligence.) In surveillance from the middle, the act of interception is
often when the spatial dynamics of these flows of media become revealed.[10]

It took Boadway some time to change his relationship to the materiality of
his correspondence. Initially, he simply tried to adjust the content of the
messages without regard for the fact that removal of a word on one side of
the paper would also remove part of the message written on the other side of
the paper. He soon started writing on only one side of every sheet of paper
(which, as a material consequence, cost more to ship from France to

California). As knowledge of the spatial flows of surveillance from the middle is revealed, people engage in tactics to avoid interception. The military learned of ways that enemy intelligence was intercepting news of its strategies and movements and thus, censored its own soldiers accordingly. When Boadway learned of ways that his letters were being censored, he responded by writing on only one side of a sheet of paper and using phrases that would avoid the military censors' notice. His response to censorship (as one mode and outcome of surveillance from the middle) was to tactically respond to the surveillance strategies of those surveilling his letters.[11]

Tactical Resistance and Infrastructural Literacy

Theorists of surveillance have argued that surveillance is produced alongside the very act of resistance used to subvert or circumvent this surveillance. As Aaron K. Martin, Rosamunde E. van Brakel, and Daniel J. Bernhard argue, "[R]esistance is not merely an epiphenomenon of surveillance—it is a basic and necessary co-development of surveillance, existing in many forms that often go unrecognized."[12] Thus, instead of counter-tactics emerging based on the modes of surveillance encountered, it can be argued that surveillance is a spatial dynamic produced with and through the very notion of resistance.[13] While such an argument is indeed compelling and pushes surveillance studies in generative directions, surveillance from the middle reveals a more complex flow of establishing resistance. Whether it be someone trying to avoid an IMSI catcher, a monarch trying to secure a letter through a wax seal, or a soldier trying to make sure his letter arrives intact to its recipient, tactics to avoid surveillance from the middle within these scenarios require that the middle be unveiled. They also require the infrastructural literacy to decode the flows of asynchronous communication and the acts of interception.

Lisa Parks argues that we must advocate for infrastructural literacy for us to engage in the politics of hidden systems.[14] Writing about infrastructure's invisibility, she notes:

> Most people are socialised to know very little about the infrastructures that surround them in everyday life, whether electrical systems, sewer pipes or broadcast networks. Not only are people socialised to be unaware of such systems; infrastructures are often designed purposefully to be invisible or transparent, integrated with the built environment, whether submerged underground, covered by ceilings and walls, or camouflaged as 'nature'.[15]

As surveillance from the middle becomes as ubiquitous as participatory surveillance on social media, the resistance to such modes of surveillance is often limited to those who move beyond a common-sense relationship to it (a relationship, I argue, that veils itself behind the everyday).[16] Once the material realities are revealed, people can find tactical modes of confronting surveillance from the middle, or "creative misuse" of these surveillance scenarios as a mode of resistance. However, this act of moving the material realities of surveillance from the middle out of the realm of common sense and into an analytical relationship that critiques and responds to such surveillance is ultimately limited to those who have the tools, access, and literacy to understand this mode of surveillance. As such, surveillance from the middle appears to predominantly benefit those who conduct the interception as opposed to those whose messages are being intercepted. Yet, as the act of interception reveals the spatial and material dynamics of surveillance from the middle, those looking for these interceptions can better respond in tactical ways.

Notes

1   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

2   Barry Levine, "Are the mysterious "interceptor" cell towers the handiwork of foreign entities?" *VentureBeat*, Sept. 18, 2014, http://venturebeat.com/2014/09/18/are-the-mysterious-interceptor-cell-towers-the-handiwork-of-foreign-entities/.

3   Rigmaiden's story was detailed on *Note to Self*'s episode, "When Your Conspiracy Theory is True," June 19, 2015, http://www.wnyc.org/story/stingray-conspiracy-theory-daniel-rigmaiden-radiolab/.

4   For more information on the IMSI catcher, see Lisa Parks' article "Rise of the IMSI Catcher" in this issue.

5   Christopher Soghoian, Principal Technologies and Senior Policy Analyst at the American Civil Liberties Union, quoted in *Note to Self*, "When Your Conspiracy Theory is True."

6   "Medium," *Oxford English Dictionary* (Oxford, UK: Oxford University Press),

http://www.oed.com/view/Entry/115772.

7   Lisa Gitelman and Theresa M. Collins, "Medium Light: Revising Edisonian Modernity," *Critical Quarterly* 51, no. 2 (2009): 1-14, 2. Emphasis in original.

8   Richard Pankhurst gestures to this tension in Ethiopia during the Middle Ages when writing was not the common form of communication except in messages delivered to very distant places. See Richard Pankhurst, "Letter Writing and the Use of Royal and Imperial Seals in Ethiopia Prior to the Twentieth Century," *The Journal of Ethiopian Studies* 11, no. 1 (1973): 179-207.

9   For a discussion of early seals for correspondence, see Thomas A. Heslop, "English Seals from the Mid Ninth Century to 1100," *Journal of the British Archaeological Association* 133, no. 1 (1980): 1-16.

10   For a similar analysis on the censorship of maps, see Trevor Paglen, *Blank Spots on the Map: The Dark Geography of the Pentagon's Secret World* (New York: Penguin, 2009).

11   For an excellent study on such tactics, see Rita Raley, *Tactical Media* (Minneapolis: University of Minnesota Press, 2009).

12   Aaron K. Martin, Rosamunde E. van Brakel, and Daniel J. Bernhard, "Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework," *Surveillance & Society* 6, no. 3 (2009): 213-232, 216.

13   I have built on this argument in my article, "Creative Misuse As Resistance: Surveillance, Mobile Technologies, and Locative Games," *Surveillance & Society* 12, no. 3 (2014): 377-388.

14   Lisa Parks, "Around the Antenna Tree: The Politics of Infrastructural Visibility," *Flow*, Mar. 2009, http://flowtv.org/?p=2507.

15   Lisa Parks, "Technostruggles and the Satellite Dish: A Populist Approach to Infrastructure," in *Cultural Technologies: The Shaping of Culture in Media and Society*, ed. Göran Bolin (New York and London: Routledge, 2012), 64-86, 64.

16   Here, I reference "common sense" in the way that Antonio Gramsci has used the word, to connote the embedded priorities of those in power as a mode of exerting such power. See *Selections from the Prison Notebooks of Antonio Gramsci*, ed. and trans. Quintin Hoare and Geoffrey Nowell Smith (London: Lawrence & Wishart, 1971).

Jason Farman is an Associate Professor in the Department of American Studies at the University of Maryland, College Park. He is also the Director of the Design Cultures & Creativity Program and a faculty member with the Human-Computer Interaction Lab. He is author of the book *Mobile Interface Theory: Embodied Space and Locative Media* (Routledge, 2012—winner of the 2012 Book of the Year Award from the Association of Internet Researchers). He is the editor of the books *The Mobile Story: Narrative Practices with Locative Technologies* (Routledge, 2014) and *Foundations of Mobile Media Studies: Essential Texts on the Formation of a Field* (Routledge, 2016). He has published scholarly articles on such topics as mobile technologies, the history of technology, digital maps and cultural geography, locative and site-specific art, videogames, digital storytelling, performance art, social media, and surveillance. He received his Ph.D. from UCLA's School of Theater, Film, and Television.