Jessica Feldman
Writing Sample

"Audio of Interest:" Contemporary State-Sponsored Eavesdropping of Cell Phone Communications

This is an excerpt of a chapter from my dissertation, which considers the effects of cell-phone surveillance for democratic social movements.

After the introduction, the first section of this chapter is a technical explanation of the cell phone and of cell phone surveillance. The second section of the chapter deals with the effects of this surveillance on social movement actors.

[Please note: Due to the current political climate in Cairo, people who would likely self-identify as "activists" in a North American context, now self-identify in Cairo as "Human Rights Workers." I use their preferred term to describe them throughout this chapter.]

"Audio of Interest:"[1] Contemporary State-Sponsored Eavesdropping of Cell Phone Communications

"People get hung up that there's a targeted list of people … It's really like we're targeting a cell phone. We're not going after people – we're going after their phones, in the hopes that the person on the other end of that missile is the bad guy."[2] – Anonymous JSOC drone operator

"I think the trust depends on what you are trusting them with. I wouldn't trust them with my cell phone. I would trust them with my life."[3] – Matta, Turkish activist and member of the Pirate Party, speaking about trust in the Gezi Park protests.

To value the security of one's cell phone over one's life might, at first blush, seem materialistic, superficial, misguided; the most confused of priorities. How could a handheld bundle of chips, capacitors, and screens be more valuable then human life? But our cell phones are access points to our identity; our personal, political, and professional networks; records of our most intimate pasts; information for imagining our political futures; and, last but not least, our private conversations. They connect us to our most precious others. A small device used to transmit voice and text over radio waves, the cell phone has become one of the most surveilled, vulnerable, and desired of objects. Control over the sanctity of one's cell phone translates into control over one's freedom of speech, of association, of mobility, and of the safety of one's contacts. These little devices have become important gateways to our political and psychological worlds.

In the previous chapter I considered the technical products that arise from an attempt to listen only for the paralinguistic, affective content of the voice. By contrast, this chapter considers state-sponsored surveillant listening as mode of listening that is focused instead on linguistic information, and the networks of actors implicated by it. This is way of listening,

---

[1] National Security Agency International Crime & Narcotics Division S2F, *untitled memo*, 2012. Accessed via Ryan Devereaux, Glenn Greenwald and Laura Poitras, "Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas," *The//Intercept*, May 19, 2014. Accessed June 21, 2014. https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.

[2] Jeremy Scahill and Glenn Greenwald, "The NSA's Secret Role in the U.S. Assassination Program," The//Intercept, February 10, 2014. Accessed June 21, 2014. https://theintercept.com/2014/02/10/the-nsas-secret-role/.

[3] Matta (pseudonym), interview by Jessica Feldman, March 5, 2015, Istanbul, Turkey, interview 49, transcript.

pioneered by national intelligence services in the hopes of finding information about those challenging the state's authority, is shifting from targeted and prosecutory, to massive and predictive. "Governance in the National Surveillance State is increasingly statistically oriented, *ex ante* and preventative, rather than focused on deterrence and *ex post* prosecution of individual wrongdoing,"[4] explains a 2008 article in the *Minnesota Law Review*.

While affective listening operates on the level of signal processing, surveillant listening operates at the level of transmission. Bruno Latour has famously described Actor-Network Theory as a means of "reassembling" and describing networks of actants who communicate in order to create "the social." He sees the *connections* between such actants as asocial and distinguishes between *intermediaries* (techniques that neutrally communicate) and *mediators* (techniques that transform or distort the message.)[5] While it is broadly accepted that publics hold a right to one-to-one, uncompromised communication, it has become increasingly apparent that this right is not unassailable: the communication channels themselves are political, and there *are* no *intermediaries, only mediators*. These conduits of transport become places for surveillant listening. And such listening does indeed transform the message, leading to self-censorship, paranoia, and a damping down on political discourse and questioning.

I focus here on a range of recent and emerging techniques for surveilling cell phone communications, which I classify by their interception points along the chain of transmission: 1) listening directly to the voice via the phone's hardware itself, 2) localized signal interception in between the cell phone and the antenna, 3) and more globalized or nationalized intervention by intercepting signals as they are sent from the antenna to the telecom headquarters. I look mainly at techniques originated by the NSA and its subcontractors and allies, as such techniques are becoming the global model for cutting-edge surveillance. Using declassified or leaked government documents, journalistic and investigative reports, and first hand accounts, this chapter traces the recent evolution and effects of these three technologies and practices.

An analysis of the effects of surveillant listening considers the ways in which betrayal or compromise at each of these specific sites has different effects psychologically and politically.

---

[4] Jack M. Balkin, "The Constitution in the National Surveillance State," *Minn. Law Rev.* 93, no. 1 (2008): 11.
[5] Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network Theory* (Oxford: Oxford University Press, 2005), 5.

As this triptych of technologies evolves, we need to think about how each approach effects the public, and their psychological, political, and associative frameworks. To do so, I take into account previous legal and theoretical literature on eavesdropping, surveillance, and privacy. This is combined with long-form interviews I performed with forty-nine activists, Human Rights Workers, NGO employees, hactivists, engineers, journalists, and organizers from New York City, Paris, Madrid, Cairo, and Istanbul, who gave accounts of their experiences of surveillance.

These actors all have articulated a commitment to democracy, and all, in some form, challenge the States in which they work. While they live under a wide range of governmental structures, and also articulate some differences in their relationships to these structures (some are more reformist, some are more revolutionary, some seek autonomy, etc.) all are advocating for democratic governance, all find themselves in oppositional relationships to their respective nation-states, and all have experienced surveillance or fears of surveillance. They are in the best position to describe the effects of this form of surveillance, both politically and personally.

Finally, I attempt to articulate what might be special about the effects of surveillant *listening*, as opposed to other forms of surveillance, and how a combination of psychoanalytic concepts and normative claims might contribute to an "ethics of listening" in this realm. The fields of Surveillance Studies and Privacy Studies have grown rapidly over the past few decades, along with the ubiquity of various forms of monitoring, tracking, and information gathering technologies. Traditionally, theories of Surveillance Studies are grounded in Foucault's critique of Bentham's panopticon. Foucault hinges a theory of modern power on this model, which operates "to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power. … the inmates should be caught up in a power situation of which they are themselves the bearers."[6] By being put in a position in which one *could* be seen at any moment, the object of the gaze self-disciplines and behaves as if he is always being watched. Surveillance Studies has largely grown out of this idea of the panopticon effect, and has focused itself heavily on the ways in which visuality produces power relations. David Lyon opens his 2007 definitive text on the subject by declaring, "Surveillance studies is about seeing things and,

[6] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan (New York: Vintage, 1977), 201.

more particularly, about seeing people."[7] Comparatively little has been written about listening to things and, in particular, to people.

While the surveillance of cell-phone metadata has become a hot topic in policy debates, security practices, and critical privacy and surveillance studies, the practice of surveillant *listening* itself is severely under theorized. Most studies of cell phone surveillance consider the collection of metadata such as geo-location, contacts, device identifiers, time and duration of calls, and the like, which can be used to locate subjects within social, commercial, and geopolitical networks and patterns. The actual practice of gathering and listening to the voice is neglected by the literature. Voice communication is historically much more well-protected under privacy law, especially in western democracies, than metadata. This is in part because the voice, to some extent, has given computerized surveillance the slip. Listening-in is time consuming, and requires human ears. Until just recently, eavesdropping was saved for highly-targeted individuals. As I discuss later in the chapter, this is changing as data storage and indexing capacities have massively expanded, and computerized listening technologies such as voiceprinting and speech-to-text software are improving. Changes in the means and techniques of surveillant listening also change the ways in which we talk and listen to each other, and the ways in which we experience the state and its powers. Any form of surveillance can be experienced as invasive, chilling, or silencing, but the effect of having someone "*listening* in" is particularly pronounced. "Eavesdropping," writes John L. Locke, in his history of audio surveillance, "has two features that make it unusually interesting…it feeds on activity that is inherently *intimate* … [and] it is *stolen* by the receiver."[8]

[Here I have cut a 25-page section of the chapter, which details the design of cellular devices and telecom infrastructures, and explains how surveillance is performed on these devices. I discuss surveillance techniques at three sites of compromise: 1) tapping into international hubs such as satellites and switching stations 2) intercepting localized communications in public space using false antennas ("IMSI catchers") and 3) hacking into the phone's microphone via the phone's baseboard. I explain the recent history of these practices and some of the legal and ethical debates surrounding these practices.]

[7] David Lyon, *Surveillance Studies: An Overview* (Cambridge: Polity, 2007), 1.
[8] John L. Locke, *Eavesdropping: An Intimate History* (Oxford: Oxford, 2010), 3.

EFFECTS

There seem to be three main effects of surveillant listening on speech, and discourse in general. The first is a so-called "chilling," or normalizing, or -- as I like to call it -- "boring" effect, which coerces populations into a kind of massive self-censorship wherein people avoid discussing anything political through technological means, especially if it deviates from the imagined dominant mentality. The second has to do with a change in the way the consequences of speech are felt over time, due to massive recording and indexing of audio files. This creates a hesitancy to speak because of fear that one's words will be used against them in some unpredictable way, in some unknown future moment. Finally, subjects repeatedly reported a concern that the cell phone jeopardized not only its user, but her entire network of contacts, making communication through network technologies a risk not only for oneself but for one's group.

These articulated effects, especially the first two, line up nicely with the "fear-based standing" definition of injury that has been used to argue against surveillance in some recent American court cases. A 2013 article in the *Harvard Law Review*, "Addressing the Harm of Total Surveillance," makes an argument for the legitimacy of fear-based standing. The authors explain that "[f]ear-based standing is the doctrine that allows fear of harm to lead to cognizable injury-in-fact for Article III standing. … The doctrine, developed in three distinct lines of cases, encompasses three ways of cognizing fear as injury-in-fact: (1) as chilling effect injury; (2) as fear of the enforcement of a statute or regulation before it is enforced; and (3) as fear of anticipated, future harm."[9]

These effects are substantial and consequential for individuals, social movements, and general populations, even if they are difficult to document. The activists, human rights workers, NGO employees, journalists, and engineers who I interviewed in the course of my research spoke frequently of the fear, anxiety, paranoia, and self-censorship caused by the specter of surveillance, sometimes describing these effects as a form of trauma. Social Movement Actors repeatedly articulate the ways in which surveillance, and threats of surveillance, cause harm to them and their groups.

---

[9] Danielle Keats Citron and David Gray, "Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards," *Harvard Law Review* F 262, 2012-2013.

Obversely, strategic policy papers on police and military counterintelligence suggest that making populations aware that they are being surveilled is an effective psychological technique to demobilize unwanted activity. My research, and others', shows that this is only partially correct: while activists articulate a deep emotional toll and logistical difficulties, many also indicate that they struggle to continue to organize and communicate in other ways, or regardless, especially in moments of crisis. General populations, however, who may have a less pronounced critique of surveillance, a less critical relationship with the state, or just happen not to be in the throes of a revolution, absolutely experience the "chilling" effect. In the following pages I will detail each of these effects, through examples from my interviews and theoretical and legal discourse. Finally, I consider how these effects operate in more pronounced or different ways as a result of surveillant listening.

Fear, Trust, and Paranoia

The fear and anxiety caused by the possibility of surveillance is deeply felt by people involved in critiquing the state. This has two effects: it can indeed impede organizers from meeting, recruiting new people, and taking action. It also has lasting psychological effects, on individuals and groups. David Cunningham and John Noakes, in their writing on the effects of surveillance on social movements, identify three main emotions, "fear, trust, and paranoia," which they claim are substantial factors in the political dynamics of these movements.[10] Social Movements are built primarily on the group: on trust and camaraderie, on bonds built through common struggles and ideologies. Threatening the ability of members of a group to bond, trust, and speak openly, can degrade these movements. An Egyptian Human Rights worker discussed these effects on the individual level:

> There was a phase in my life where the telephone was *not safe*. It still isn't. Every time I speak on the phone, I always bear in mind that someone might be listening in, which conditioned me to always take extra precautions for the longest time, to the extent where I felt entrapped, I felt trapped for a while. … Um, which, in itself fueled lots of trauma and lots of issues that I think not just me, but lots of people, have to work through. … I have trouble writing about my emotions, for fear that someone might find it,

[10] David Cunningham and John Noakes. ""What if she's from the FBI?" The effects of covert forms of social control on social movements," *Surveillance and Governance: Crime Control and Beyond*. Published online: 09 Mar 2015; 175-197. http://dx.doi.org/10.1016/S1521-6136(07)00208-4

> whether someone on the other side, or someone on my side. It's something that I'm currently working on to try to resolve on a personal level.[11]

Other activists and organizers in Egypt and elsewhere have expressed feelings of fear, paranoia, and "craziness" as a result of surveillance concerns. Another organizer from Cairo working on women's rights explained, "It can make you crazy. When do you stop? You have to constantly think about what is dangerous for you."[12] A French communist also described a lasting shift in mentality that occurs as a result of thinking about surveillance:

> After our friends got arrested, every time I texted, I was thinking, "are *they* reading it? I was thinking Big Brother, etc. I was telling a friend, maybe *they* might be watching. … You can't know that *they* found you interesting until it's too late. Very often if you think you're being surveilled, you sound paranoid. And often you will be. There are moments when you become aware of it, and then it fades away. It's such a general perspective and then it fades away, recedes. … Then maybe a point comes when it is part of your mental state for good.[13]

This shift in mental state can scale up to the level of the group, affecting the members' ability to trust and work with each other, and deterring association and actions. The paranoia and the "chilling" go hand in hand. One experience of infiltration by a spy can damage a group for years to come. In this case, the leaking of information is secondary to the loss of safety and trust that the group requires in order to operate. A Spanish activist explained: "Spies are a real problem. At the beginning of 15M[14] we trusted in everyone. But then, you have one bad experience with a

[11] Nadir (pseudonym), interview with Jessica Feldman, February 11, 2016, Cairo, Egypt, interview number 34, transcript.
[12] Esther (pseudonym), interview with Jessica Feldman, February 09, 2016, Cairo, Egypt, interview number 27, transcript.
[13] Paul (pseudonym), interview with Jessica Feldman, January 3, 2016, Paris, France, interview number 13, transcript.
[14] 15M is a name for the anti-austerity social movement that originated in Spain in 2011, marked by massive public demonstrations and occupations of squares on the 15th of May.

spy, and two weeks later you start thinking your friend is a spy. This is a really big problem for groups."[15]

The fear and paranoia that come with the awareness of surveillance may not be simply an unfortunate byproduct of the surveillance state, it may in fact be an intended consequence. Activists and security strategists alike attest to this. In a 2014 article in *New York University Law Review*, Samuel Rascoff, the former director of intelligence for the New York City Police Department, details the philosophy and goals of "new deterrence," which seeks to "manage terrorist risk through the potentially widespread, deliberate employment of fear."[16] According to Rascoff, this approach relies on "government omniscience and omnipotence" in order to frustrate the enemy, using fear to "serve a core strategic purpose." He cites notification of surveillance as a prime example of this:

> Regarding the administration's surveillance of financial transactions through the SWIFT clearinghouse,[94] Treasury officials "injected [broad discussions of Financial surveillance] into any testimony" as "part of an explicit communications strategy to explain what [they] were doing without revealing the details of the methods [they] were using."[95]

Such a tactic need not be limited to terrorists or money-launderers. Governments also are interested in instilling fear and distrust in other "enemies of the state" such as activists, or, in some states, Human Rights advocates. Nadir, a Human Rights worker in Cairo told me:

> Here, it is state-sponsored fear, where they want you to think That you're being monitored, even if you're not being monitored. I've noticed it especially since post-2013, where everyone suddenly started feeling more paranoid than they ever felt before, everyone feels like they're under threat. Our increased knowledge of all of these new technological means that are being developed, our knowledge of these contracts that are being signed between the Ministry of the Interior … and international companies that are developing different software and algorithms for monitoring …. and this is now public information. And it's intended to put you in that frame of mind. And I actually felt it, even though I'd grown up

[15] Marcos (pseudonym), interview with Jessica Feldman, January 25, 2016, Madrid, Spain, interview number 23, transcript.
[16] Samuel J. Rascoff, "Counterterrorism and New Deterrence," *New York University Law Review* 89, no. 830 (2014): 851.

> with it for so long. It still gets you a little more paranoid. Especially when lots of your friends are suddenly all being taken to prison.[17]

In some cases, this works: the fear of surveillance is enough to stop association or actions altogether. In some cases, actually, it does not. The more successfully repressive the regime, the more chilling the effects of surveillance. In western "democracies" such as the U.S. and France, most of the activists I interviewed did not cite surveillance as a deterring factor in organizing, although they did feel that the effects of fear and paranoia were damaging to the psychology of the groups and individuals involved. In Spain, where new laws have been passed increasing jail time and fees for organizers of unpermitted public actions, activists have become more leery of taking such actions for fear that the organizers will be identified. As one Spanish activist told me, "In December, we didn't do anything spectacular because we were worried about surveillance. We talked with a lawyer for 15M, and he recommended that we stop the activity because it was too much of a security danger for us. It's not possible to pay that much money."[18]

In the Middle East, the stakes are higher. Ragna, an employee at an Egyptian NGO focused on gender and sexuality expressed a feeling of desperation at the best way to continue working in light of surveillance. "It's very difficult doing anything. There are lots of disappeared people, killing, massive torture. I really don't know what is the best to do."[19] Nadir described the situation leading up to the Egyptian Revolution of 2011, "people were so worried that they were either under surveillance, or that they were going to be placed under surveillance, that lots of people wouldn't even engage in anything political in the first place. So it was very difficult to mobilize. I had people that didn't want to come over to my house because they were worried that they'd be placed under surveillance."[20]

However, at the moments when the regime starts to crack apart, the fear and paranoia dissipate. There seems to come a point when activists, even those facing the greatest threats, recognize that everyone is being harassed, stop caring, or refuse to succumb to the fear. In Cairo, a legal researcher at a university told me a story about receiving a call from the Ministry of

---

[17] Nadir.
[18] Javier (pseudonym), interview with Jessica Feldman, February 1, 2016, Madrid, Spain, interview 27, transcript.
[19] Ragna (pseudonym), interview with Jessica Feldman, February 7, 2016, Cairo, Egypt, interview 31, transcript.
[20] Nadir.

Interior, telling him to stop his research. He responded, "or what?" and then hung up the phone. He explained that his reasoning was that they would either kill him, or not kill him, and he could not live in constant fear of it, he had to do his work.[21] Others articulated similar forms of "psychological resistance," even when they were sure they were under surveillance. Ragna explained, "when you talk on the phone, you know police are listening. After a point you are like, fuck it, I'm using my phone."[22] Esther, another Egyptian human rights worker, expressed similar sentiments: "I don't want to be part of the cycle of being afraid we are being surveilled all the time. I know we are, but I can't live this way, thinking ten times before I send an email. I'm not going to change my life. It's not safe anyway. I want to enjoy life."[23] She also told me a story about writing letters to friends in prison, and including little notes and jokes for the officer who was most definitely reading the letters. "It's a funny thing, you know, you have a whole relationship with this third party! I don't know him, but I'm sure he's very interesting. … You have to have a sense of humor or it gets to dark."[24]

In these cases, there are some for whom the chilling effect isn't working. There is no paranoia: they are not afraid of the possibility of surveillance, in fact, they are quite certain of it. They are also aware that everyone in their community is subject to surveillance, and there is a common sense of rejection of it as a legitimate gesture. In Esther's case, there is even a breakdown of the "us-versus-them" barrier as she decides to communicate and joke with the unknown officer on a more intersubjective level.

If chilling is a feeling and practice of isolation, hinged on shame and insecurity, then a sense of solidarity and communal rejection of the state's authority can override the chill. Elizabeth Stoycheff's findings support this. In a 2016 article in *Journalism & Mass Communication Quarterly*, Stoycheff studied how the perception of mass surveillance, combined with the conviction that such surveillance may be justified, effects the voicing of politically dissident views online. Subject groups that felt that surveillance was either "justified" or "tolerable" exhibited sharp drops in their willingness to speak out in hostile climates under surveillance. However, the subject group that felt that surveillance was "*not* justified" barely exhibited any

---

[21] Mohammed (pseudonym), interview with Jessica Feldman, February 6, 2016, Cairo, Egypt, interview 30, transcript.
[22] Ragna.
[23] Esther (pseudonym), interview with Jessica Feldman, February 10, 2016, Cairo, Egypt, interview 33, transcript.
[24] Esther.

change in their willingness to voice dissenting opinions when under surveillance.[25] Nadir associates this with a sense of empowerment that comes with collective action, and a collective willingness to reject the state:

> 2011, specifically the 25th of January, broke a certain barrier that decreased people's fear of surveillance. Because, while surveillance at one point in time seemed to be the worst case scenario, now you're being shot at and killed, and the police state seems to be collapsing, so … yay. … When there are more people on the ground, there is less paranoia. … you're marching in the streets, and those around you are in the same group of activists, you know, these are people who are in the street for the first time, they are prepared to die or be arrested. So that almost alleviated the fear.[26]

Boring

But revolutions are extraordinary, exciting moments. These are examples of mass movements in large cities organizing to overthrow oppressive regimes. Surveillance has a more troubling effect as it creeps into the daily lives of subjects of more docile and allegedly democratic states: people become boring, and that becomes normal. This poses a threat to democracy, insofar as it relies on the regular engagement of the people in political life. Theories of the democractic public sphere, from Rousseau to Habermas, hinge themselves on and free discourse and public assembly: listening and speaking freely, experimenting with positions and possibilities, playing the "devil's advocate," challenging the current system, making mistakes, changing one's mind, and trying out ideas and processes that might not be good ones in order to arrive at better ones. This is interesting. In a state of emergency, this kind of activity can be enough to flag one's speech as "audio of interest" and to subject her to eavesdropping. The common defense against this threat is to "act normal."

The idea of "normal" appeared over and over in interviews with Social Movement Actors. This term was used in two ways. The first was to describe state surveillance: either speaking about how surveillance had become "normal" or about how the state of emergency was not "normal" democracy. The second was to describe the subjects themselves, and their attempt to maintain the appearance of being "normal" in their communications, so as not to be subject to the fallout of surveillance.

---

[25] Elizabeth Stoycheff, "Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring," *Journalism & Mass Communication Quarterly* March 8, 2016.
[26] Nadir.

In a meeting with a group of environmental activists in Paris, one woman told me, "two days ago I was doing something with other activists. One of them, I didn't think she could be surveilled, but yet she had been. My conclusion is that it is normal to be surveilled in France."[27] Similarly, an Egyptian Human Rights Worker, and the son of a dissident politician, told me:

> [It's] been part of my upbringing, as well as part of our daily lives now. It's completely normal, halfway through a conversation to be like, "let's just talk in person." And that instantly triggers that, uh, "yep, we might be … let's just be safe and talk in person. And it's been that way for years.[28]

A Turkish activist and scholar who advocates for the use of privacy tools, said:

> They are watching all the people, but activists especially. If I were a normal man, I'd use these tools too, because I know they are watching. Some young and old people went to prison just for posting things. The government can collect everyone. They want people to know that they are watching all the people, and if you say something you can go to prison. They want us to know that.[29]

Surveillance is no longer thought of as targeted, but as part and parcel of digital communication in these states. The response to this is to appear as "normal" as possible. In this case, "normal" means apolitical: users do not visit political or controversial websites, use encryption tools, participate in public protest, or discuss anything controversial over the phone. When surveillance becomes normalized, "normal" behavior becomes boring.

One activist and technologist from New York City told me:

> I started noticing about three to four years ago that, umm, so, long story short: there's a company called cyveillance that is trying to anonymize themselves. I noticed weird traffic on the sites [I was visiting.] I looked into it, and they are contracted by NSA. They show up everywhere I go. I tried all sorts of things, and they are everywhere. They are tracking me for everything and who knows why … I am a kind of middle-of-the-road person when it comes down to it. … If there is that much surveillance, why bother? … I'm not doing anything that requires me to use Tor … I've given up because I think it flags me. *The best thing I can do is be as boring as possible all the time*. That's not hard. …

---

[27] Group interview with Jessica Feldman, January 11, 2016, Paris, France, interview 15, transcript.
[28] Nadir.
[29] Peter.

> I've come around to thinking it's easier to be a needle in a haystack right now, because using encryption flags you as weird.[30]

A French journalist who works with wikileaks explained that he only encrypts a small portion of his communications, which he does his best to keep under the surface. "Most of my telcos are in plain text, as I'm also aware that it's almost impossible to be secure all the time: everybody makes mistakes, and I've preferred to learn how to secure my communications when I need to than to try to be secured all the time … for the past 15 years, I lived with the fact that I could be spied on."[31] A Kurdish-rights activist explained, "if everything is encrypted, "they" will look at it. [I] keep a layer of "normal," and keep a layer that is not."[32] This behavior is not exclusive to digital communication, either. In an interview with "Ciudadano Pásalo,"[33] s/he explained that their tactic on the night of the illegal protests that s/he initiated was to "act like I was a regular person,"[34] on the phone, on the internet, and in public and private space.

This attempt to speak "normally" is generally called the "chilling effect," which describes a quieting of marginal viewpoints and public debate with regards to politically controversial or sensitive topics, especially with regards to anything that questions those who initiate the surveillance (that is, the state or the corporation.) The term entered American legal jargon in a 1952 U.S. Supreme court ruling involving required loyalty oaths for state employment. The court ruled that these oaths, which required the professors signing them to affirm that they had never been a part of any "communist front or subversive organization," were unconstitutional and had "an unmistakable tendency to chill that free play of the spirit which all teachers ought especially

---

[30] Becca.
[31] Anonymous, email to Jessica Feldman, December 26, 2015.
[32] Juan (pseudonym), interview with Jessica Feldman, January 26, 2016, interview 20, transcript.
[33] Ciudadano Pásalo is Spanish for "Citizen Pass-it-on." This is the pseudonym given to the person who is credited with initiating a series of nation-wide illegal protests following the Atocha bombing in March 2004, which led to the unseating of the right wing party. The protests were called for in a text message that Ciudadano Pásalo sent to seventeen people, who then sent the message out to a handful more people, who continued to "pass-it-on" until it entered the media. By that evening there were massive protests in Madrid, Barcelona, and Bilbao. Ciudadano Pásalo believes that people we angry and eager to protest, and describes the message as something that "threw a match in gunpowder." This occurred on the day before elections, "reflection day," when it is illegal to have any public political events.
[34] Ciudadano Pásalo (pseudonym), interview with Jessica Feldman, February 2, 2016, interview 27, transcript.

to cultivate and practice."[35] Today "chilling" is related to not just to a suppression of free thinking, but also to fear of isolation from mainstream culture.

The idea that surveillance has a silencing effect is widely understood in political communities. In Spain, the new surveillance law, "Ley Secquridad Ciudadarna," ("Law for the Security of Citizens") is now called the "Ley Mordaza" ("Gag Law") by activists.

Protest against the "Ley Mordaza" in Spain, Spring 2014

Andrew Song, a privacy researcher at Harvard Law School, argues for a new term to describe this effect, the "fishbowl effect." It is not just that socially valuable speech is "chilled," he says, but, more so, we no longer really engage in anything that could label us as targets for the surveillance apparatus:

> I prefer the term "fishbowl effect" to refer to the inhibiting effect of loss of privacy. If we lived in a transparent glass bowl as goldfish do, we might end up doing what goldfish do — which is not much of anything.[36]

[35] Schauer, Frederick, "Fear, Risk and the First Amendment: Unraveling the Chilling Effect" (1978). Faculty Publications. Paper 879. http://scholarship.law.wm.edu/facpubs/879

[36] Andrew Song, "Technology, Terrorism, and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches," The Berkman Center for Internet and Society, Research Publication No. 2003-04 (5/2003), 15.

I call this the "boring" effect -- doing and saying not much of anything in order to appear uninteresting to the state. It is important to note, however, that it's more of a veneer of boring than true boringness. Beneath the surface, people are actually interesting: activists find ways to talk and meet, and people use pseudonyms and encrypted communications, and visit websites anonymously using Tor and VPNs. The real danger of "acting" normal is the *concealing* of dissent, diversity, and discourse, and how this affects the public realm.

Under these conditions, we no longer have a sense of what the public truly thinks, in fact, we no longer have a democratic public. "Marginal" or "extreme" viewpoints may be more widely accepted or considered than is represented by communications technologies. Taken to its logical conclusion, if a population is fastidiously "boring" itself, the margins of acceptable expression will become narrower and narrower until there is not room for political discourse at all. Rogaway worries that the NSA's obscure eavesdropping algorithms mean that "it will be impossible to understand the contours of the surveillance apparatus by which one is judged. All that people will be able to do is to try your best to behave just like everyone else."[37]

The real political fallout of this "false boring" is that we no longer know what is normal public opinion, and there is no space to participate in negotiating this. Georges Canguilhem's 1989 printing of *The Normal and The Pathological* theorizes that we only know what is "normal" because of deviations from it. Canguilhem traces the emergence of the category of "normal" to the emergence of standardized measuring devices, and then statistics. Deviance, he says, can only be perceived when contrasted with "norms," and norms themselves are the result of a negotiation aiming to articulate the most commonly occurring and convenient quantities.[38] If everyone is "acting" normal, there can be no negotiation among viewpoints. The marginal figure, therefore, is essential to inciting discussion over normative claims, to arriving at an ethics and politics through democratic discourse.

Recording our Guilty Futures

Mladen Dolar has written "democracy is a matter of immediacy, that is, of the voice."[39] With the advent of massive data storage, such as the SOMALGET system, the temporality of

[37] "New Snowden Files …"
[38] Georges Canguilhem, *The Normal and the Pathological* (New York: Zone, 1991).
[39] Mladen Dolar, *A Voice and Nothing More* (Cambridge, MA: MIT Press, 2006), 109.

telephonic speech changes. Speech, generally experienced as fleeting and unaccountable, becomes something to which we are "held" when it is recorded. This is something speech-writers, public figures, and performers are used to and prepare for. "Normal" citizens engaging in unscripted conversation, however, do so in order to hear each other's ideas, information, and viewpoints, to try out and develop concepts and plans, and to share feelings on the fly. Phone calls are places where one can be unofficial, intimate, off-the-record, and unsure. Such forms of conversation are essential to the creative generation of everything from political plans to romantic relationships, new friendships and old family ties, artistic collaborations and financial negotiations.

Programs like SOMALGET, which record speech and hold it for 30 days, or indefinitely, change what it means to speak. When our conversations can be used against us at any point in the future, we start to speak in a much more restricted manner. Instead of living in the realm of the improvisatory, creative, and dialogic, telephonic speech becomes something that can come back to haunt us, and therefore it becomes carefully constrained. The temporality of speech and the consequentiality of guilt are in a close relationship here. These storage programs allow for our spoken thoughts, in the current moment, to count as evidence towards our future guilt. Whereas guilt traditionally is related to a past action, in this case the very act of speaking, of thinking out loud, can be used against subjects in the future as evidence of guilt.

Speaking about State surveillance, an Egyptian artist/technologist articulated a direct opposition between being recorded and cultivating her creativity:

> I don't think an average Human Rights person hasn't had at least one nightmare of being chased and tortured. But the fact that digital security is not sticking to the concerns of people in general … this makes you worried, not just for yourself, but for your contacts. And for what you did and said in the past. I don't want to take on the feeling of paranoia that comes with knowing about this. I hope I can cultivate the curiosity that comes with hacking. It's hard for me to deal with the fact that we are constantly recorded. If it's not the Egyptian state, it's the "holy grail" of the NSA.[40]

[40] Hanna (pseudonym), interview with Jessica Feldman, February 17, 2016, Cairo, Egypt, interview 34, transcript.

That is, being *recorded,* in particular, affects one's ability to be creative. Hackers operate by making mistakes: taking thing apart, testing them out, accidentally breaking them, rebuilding them, experimenting, and tweaking. This kind of work relies of the ability to try things out before "going public" or creating a final product that is recorded, documented, or put into circulation for use. The recording of speech changes its creative valences – it is no longer a place for exploratory conversations, but instead something to be carefully guarded with an eye towards future liabilities.

Similarly, an Egyptian musician who was active in the revolution told me about the effects of having his speech recorded by the government, and how he deals with it by carefully scripting what he will say so that he can plan for its potential consequences:

> … anything that I do say that could be incriminating, at least I have the upper hand of *knowing* that I have said this, that it can be used against me, and I have a backup plan of what is going to happen if it is used against me. So it's a lot of planning, planning for the worst case scenario, strategizing. Living the worst case scenario in your head, so as to prepare you in advance for an almost inevitable damage that will be caused by the government.[41]

In Egypt this is a very salient threat, both in terms of personal safety (not being arrested) and psychological safety (not being humiliated.) There is an Egyptian "news" series called "The Black Box," in which the government supplies the show's host with recordings gathered by surveilling activists' cell phones, and the host mocks them and uses their personal communications to humiliate them.[42] Although the NSA's style is a bit more subdued, both states are using the notification of surveillance as a form of deterrence, and the consequences are similar: an unwillingness to speak playfully, intimately, or politically over the phone for fear of future guilt, prosecution, or humiliation.

---

[41] Nadir.
[42] Salma (pseudonym), interview with Jessica Feldman, January 12, 2016, Cairo, Egypt, interview 28, transcript.

As a Spanish activist and sound artist explained, power lies in who can decide when to record: " … the real thing is, who can press the red button? Can they stop or start it? This is why I want to hand the recorders to people."[43]

"Contact Chaining" and the Sanctity of the Other

Another very commonly articulated concern regarding cell phone surveillance has to do with the nature of networks: people are worried about compromising their contacts. In fact, this worry was as important as concerns about personal safety. Whereas massive recording practices gather the content of the speech, concerns about the safety of one's network has more to do with protecting metadata. In democratic activists groups especially, the protection of the group does not hinge on the survival of the individual or the protection of the individual body, but the on the protection of the network: of the contacts, of the others. As Matta articulates in the opening quote, trusting someone with your cell phone is a bigger deal than trusting someone with your life, because the cell phone leads to other's lives. Democratic activist groups, especially those engaged in non-violent protest, practice a form of politics that prioritizes the "people" over the individual in order to come to political decisions and directions. For this reason, networks are particularly precious.

Organizing methods during public assemblies recognize this. Over and over, I was told that the primary security concern in public actions was to protect the person who held the cell phone through which messages were broadcast – not necessarily because of her broadcast authority, but because she held the information of all the group members. "In big events, the policy is always to take care of the people with the phones,"[44] one ecologist activist told me. "You need to have somebody always taking care of the phone carrier[45]," said a member of a French socialist organization. In large actions such as protests, especially if they are illegal, a small group of people carries phones and coordinates activities, while other participants do not, for fear of being arrested and having their phones confiscated.

Therefore, even in groups that aim to operate without hierarchies, the "people with the phones" take on leadership positions, because they have the greatest network power. The carriers

[43] Carlos (pseudonym), interview with Jessica Feldman, January 21, 2016, Madrid, Spain, interview 19, transcript.
[44] Michel (pseudonym), interview with Jessica Feldman, January 17, 2016, Paris, France, interview 16, transcript.
[45] Eric (pseudonym), interview with Jessica Feldman, January 18, 2016, Paris, France, interview 17, transcript.

of the phones are the central nodes through which the group is constituted. This poses a problem for actions such as protests, which are under localized, immediate surveillance (e.g.: IMSI catchers), because it is so easy to identify these people. "The police know who is the leader of activism because they are the nodes,"[46] explained a Spanish activist who was involved in 15M. Increasingly, those in "leadership" positions are faced with greater punishments for organizing public actions. In France this can take to form of house arrest or jail time. In Spain, there are very large fines associated with participating in unpermitted public protests, and these fines can be increased 100-fold, up to €601,000, for the people who organize the actions.[47]

> It's easy to know who is the leader … this is the problem. But we have to communicate at every demo. But the leader doesn't have the money to pay [the fines]. But the police are paid to spy. They're going to see what you are doing. But you're going to do it anyway. If you're in a normal democracy, you are protected. But this is not the case in Spain.[48]

Increasingly, this is not the case in many places, including States that claim to be democracies. This creates in the populace a particular kind of paranoia and fear of freely associating using network technologies. A gender-rights activist in Egypt told me: "The people you are talking with might face problems ... The first thing, if you get arrested, is they take your phone. They took one of my friend's phones. The police called whoever was last in his phone and tried to get her to meet "him." I was talking with him a few minutes before [his arrest.] I was very paranoid. The problem is you are always feeling insecure, being watched."[49] This particular paranoia is about being part of a group: losing control of your contacts, or being in danger because one of your contacts is. Carrying a phone means carrying the fear that you could hurt your loved ones and comrades. An activist in France articulated the same thing from the perspective of the one *with* the phone: "The worst thing is you end up very paranoid. Maybe I'm surveilled and then I'm giving up info about people I am in contact with."[50]

<u>What is special about listening?</u>

---

[46] Ajax.
[47] Amnesty International, *Spain: The Right to Protest Under Threat*. London: Amnesty International Publications, 2014. Accessed April 2016. http://www.amnesty.eu/content/assets/Doc2014/Spain_formatted_24_03_14.pdf
[48] group interview, January 11, 2016.
[49] Salma.
[50] Paul.

These are problems with any network technology, especially with mobile ones. Our phones do many things other than transmit voices. But there is something special about listening that makes it both necessary for democratic discourse, and also the most invasive form of surveillance.

In a 2007 study on varying forms of workplace surveillance and their perception by 246 workers, telephonic eavesdropping was compared with computer monitoring and visual surveillance (video cameras, etc.) Workers were polled regarding their perception of these various techniques in terms of procedural justice, interpersonal justice, and privacy. Eavesdropping ranked the lowest in terms of both procedurally just and interpersonally just techniques, and the highest in terms of felt privacy violations. The authors of the study attribute this to telephonic eavesdropping's capacity to monitor non-work related communications.[51] Indeed, the phone is often used to call family and friends, make doctor's appointments, pay bills, and other personal activities. I would posit that this "non-work" information that is contained in vocal conversation is indeed unique: listening-in captures things that computer and visual surveillance cannot capture: the immediate, the affective, and the intimate. For this reason, conversation is an important aspect of building interpersonal relationships, trust, and understanding. If these spaces are compromised, so too is the subject's ability to safely share their self and to build intimacy and camaraderie.

In my survey of 49 activists in New York City, Madrid, Paris, Cairo, and Istanbul, subjects responded that the most important medium for communication in organizing and during a protest was voice. It was considered the most immediate, the most reliable, but also the most tightly linked with identity and integrity of message. Nadir, from Cairo, told me:

> I prefer the voice. If I every feel that something's fishy, I'll call the person. I'll ask for voice verification. "Ask for voice verification" sounds like a very procedural matter, but I'll just call the person to make sure that it's actually them. Ironically, I do it with my mother a lot. Lots of the time, if there's a weird message from my mother. Or with specific friends. Very short, ominous messages concern me, and I end up basically responding by calling rather than texting.

[51] Laurel A. McNall and Sylvia G. Roch, "Effects of Electronic Monitoring Types on Perceptions of Procedural Justice, Interpersonal Justice, and Privacy," in *Journal of Applied Social Psychology,* 2007, 37, 3, pp. 658–682.

The voice is linked to identity and cannot be spoofed in the way that texts can. Calling allows subjects to be sure of this, and to clarify ambiguities in tone that may not be clear from texts.

However, the uniqueness of the voice becomes a site of surveillance as well. In Turkey, the leading mobile phone service provider, TurkCell, encourages its users to submit to voiceprinting in order to receive assistance form call centers. The company, whose slogan is "Turkcell knows me by my voice," has the voiceprints for at least 10 million customers.[52] Not surprisingly, activists and journalists in Turkey report that telephonic eavesdropping is the main form of surveillance to which they are subjected. According to a group of journalists working with Dokuz8Haber[53], a citizen journalist network in Turkey, 90% of court cases against political figures are based on telephonic surveillant listening.[54] A Turkish engineer and activist I spoke with explained that voice was the best way to communicate quickly during protests, but that it also provided the most personal information to the State. "If you speak in terms of oppression, … if your device gets arrested and there is a voice message, it is easy to identify who is speaking."[55] Additionally, the TiB (Turkish Telecom Authority) has placed notifications all over the country notifying people that public spaces are both audio and video recorded.[56]

Privacy and the Voice

In 1928, U.S. Supreme Court Justice Louis Brandeis delivered a dissenting ruling in a case against government surveillance. This text has become a grounding argument for the right to privacy, framing it as a fundamental human right, something necessary to "happiness," that most sacred of American values:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone – the most comprehensive

[52] "Turkcell a global leader in voiceprint 'harvest'," *The Daily Sabah*, October 14, 2014, accessed May 30, 2016, http://www.dailysabah.com/nation/2014/10/14/turkcell-a-global-leader-in-voiceprint-harvest.
[53] Dokuz8 has been shortlisted for the 2016 Freedom of Expression Award by the Index on Censorship.
[54] Dokuz8 group interview with Jessica Feldman, February 28, 2016, Istanbul, Turkey, interview 44, transcript.
[55] Odin.
[56] Dokuz8.

> of rights, and the right most valued by civilized med. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever means employed, must be deems a violation of the Fourth Amendment.[57]

Here Brandeis links the protection of one's privacy with the protection of one's thoughts and feelings. What is most important here, although it is rarely emphasized, is the idea that privacy is necessary for the *pursuit* of these facets of happiness. That is, privacy is not only necessary to protect ideas, feelings, and connections that already exist, it is a necessary condition for the generation of these ideas and feelings. This is a psychological argument with political consequences: the loss of privacy affects our ability to create new ideas, technologies, and communities, and to act and think collaboratively about these.

An engineer working at a Human Rights NGO in Cairo, and who had worked on the communications team in Tahrir Square, articulates clearly that privacy is a necessary condition of creativity and humane living:

> You can't be creative without a layer of privacy and authority over your data. If you are in a public square and people are watching you, versus if you are in a room and trying, you can just kick ass and try. If you are under many restrictions and deadlines, you can't try. It doesn't mean you are doing something wrong, it means you are doing something different. … Privacy is the core value for the rest of human rights. You can't have the other rights or liberties (expression, religion, sexual) without the privacy to do that in a free manner.[58]

How do these new surveillance practices and technologies, in their particular implementations, effect a population's ability to develop their rights and liberties, to pursue "happiness"? Massive audio capture and recording, like MYSTIC and SOMALGET, pose an ever-present threat. In this case, the power of the surveillance is in its totality and in the threat of *future listening*. Speaking becomes something that resonates far into the imagined future. While the panopticon is described as a disciplinary measure, which kept people behaving compliantly in the moment, this new kind of recording-without-listening keeps people from thinking out loud

---

[57] Justice Louis D. Brandeis, "Dissenting Opinion," *Olmstead v. United States.* 277 U.S. 438 (1928). http://www.fjc.gov/history/home.nsf/page/tu_olmstead_doc_15.html

[58] Ahmed (pseudonym), interview with Jessica Feldman, February 16, 2016, Cairo, Egypt, interview 35, transcript.

in the present, for fear that it could be used against them in the future. Instead of discipline, this creates self-censorship and anxiety, which stifles speech for fear of "how it could be used against you," rather than fear about the actual information being leaked and the loss of its contextual integrity in the moment. This causes a form of speech that is more scripted and carefully contained. Speech cannot be a place to experiment with political ideas, feelings, or plans, because the fact of recording fixes one's position. If speech is midway between ideation and action, the recording of speech makes it more definitive, something for which subjects are held responsible. Creativity and experimentation then must retreat to the realm of imagination and fantasy, not to be articulated in words. Yet we know that speaking something is the first step to bringing it into being, and that without speech, in isolation, we forget to develop our ideas and imagination. They atrophy and are forgotten. Surveillant recording of speech has the effect of chilling not just our discourse, but our imaginations.

IMSI catchers, on the other hand, intercept the signal locally in real-time, and are designed to travel around to surround protests, rallies, and the like. This *circulating, just-in-time listening* has more direct effects on public assembly and solidarity networks. In this case, listening and meta-data monitoring happens based on location and activity, and therefore targets particular political and social networks. In this case, intercepted information can be descriptive of the movements and actions of the group in the moment. This creates concerns among groups about compromising *the other* – about the danger of connection and affiliation. Secondarily, this also keeps assembled groups from using cell phones in order to avoid interception of their communications in terms of their plans and movements.

Finally, devices like roving bugs and sleeping chips, whether actual or notional, have the effect of provoking anxiety at a more intimate location: the mobile phone is kept close to the body and moves with the subject through their daily life. While programs like MYSTIC present a threat to telephonic speech, roving bugs are present whenever the phone is present, and could be listening at any time. This is less about *future listening* and more about *potential listening* – the device could be listening at any moment, to any sounds. Carrying around a cell phone in this case means carrying around a sensation of betrayal and distrust for one's personal objects. Instead of acting at the level of corporate infrastructure, this form of intervention occurs on a much lower technical level – in the hardware itself – and therefore is experienced as ever-present but not omni-present. Instead of listening from high above or deep below – from the cloud, the

satellite, the fiber-optic cable -- this eavesdropping happens in our hands, our purses, and our back pockets, creating an nagging, constant, low-grade sense of distrust of the "personal" field surrounding the voice.

[end excerpt.]