Under Surveillance: Technology Practices of those Monitored by the State

Pedro Sanches, Vasiliki Tsaknaki
Media Technology & Interaction Design
KTH Royal Institute of Technology, Sweden
sanches@kth.se; tsaknaki@kth.se

Asreen Rostami, Barry Brown
Department of Computer and Systems Sciences,
Stockholm University, Sweden
asreen@dsv.su.se; barry@dsv.su.se

ABSTRACT
This paper documents the experiences of those living under state surveillance. We interviewed our participants about how they lived under threat, and how it changed their technology practices. Our participants spanned three groups - journalists who reported from countries where their activities were illegal; activists who took part in civil disobedience, and individuals who worked in illegal activities that would have likely led to prosecution. In our analysis we cover four themes: first, 'the imagined surveillant'. Second, the danger and dependencies of technology use, third, their coping strategies, and lastly how belonging to a group can protect but also expose. In our discussion we cover how we can design for dissidents, and how to deal with the difficult questions this raises. We conclude by advocating for research that takes into account a critical view of the state in HCI and more broadly for an anti-surveillance stance in the design of technologies.

Author Keywords
Surveillance; dissidents; state;

CSS Concepts
• Human-centered computing~ Human computer interaction (HCI) ~ Empirical studies in HCI;

INTRODUCTION
As our lives have become ever more digitised, so the details of those actions are increasingly traceable by the state. Many mundane and harmless activities create online data trails that are obtained, tracked and analysed by varying state agencies. While there have been extensive regulatory efforts to curtail this surveillance, it has also become a standard part of police work. Under various motivations such as the prevention of terrorism, the maintenance of state secrets or the protection of public order, governments around the world – both democratic and despotic - maintain extensive systems of surveillance of their citizens [28].

CHI 2020, April 25–30, 2020, Honolulu, HI, USA.
 ACM ISBN 978-1-4503-6708-0/20/04...$15.00.
DOI: https://doi.org/10.1145/3313831.

Surveillance has been an extensive subject of investigation in the field of "surveillance studies"; where issues around the political ethics of surveillance, as well as the development of new technologies of surveillance have been extensively debated [19,27,28]. What has been much less investigated, however, is how users respond to state surveillance, particularly when performed by security forces (c.f.[44]). Researchers have shown that modern surveillance is best understood as an assemblage [19] of corporations, states, institutions and the general population, where data is collected at various points and concentrated in centres of calculation (e.g. police databases, corporate databases, etc.). This has been studied from many perspectives, e.g. when states manage populations in welfare systems [12], or for public health reasons [8,39,40], in emergency systems [6] or under the umbrella of surveillance capitalism [24,50], when data is sold for profit. Surveillance is known to reproduce existing inequalities, disproportionately affecting already disadvantaged groups [5]. Here we focus particularly on people monitored by security apparatus of the state. For our participants, the security forces are a crucial agent alongside private telecommunication operators and social networks. Research has shown that security forces are able to mobilize data through means usually unavailable to most stakeholders (e.g. through data fusion centres [32]). A distinctly social computing topic then arises: *How do those who are under state surveillance change their technological practices?* For this paper we sought to investigate how people 'under surveillance' used technology in different ways, and how online and offline practices changed in such circumstances. Our aim is to bring into the discussion the experiences and practices of a group who have been mostly absent from HCI research [41,43].

The group we were interested in was those who have obtained proof of being under surveillance and had reasonable suspicion that they were still under surveillance. For shorthand we refer to these individuals as 'under probable surveillance'. As we will discuss, even being under surveillance for a short period can have lifelong effects. Our participants are journalists who reported from, or had reported from, countries where those activities were considered illegal; activists who took part in civil disobedience or protest operations, such as disrupting government infrastructure; and individuals who worked in illegal activities that would have likely led to prosecution if caught. Our recruited participants come from different

countries in Europe and Asia, and a majority lived under democratic, non-authoritarian regimes, as our goal was not to document solely surveillance under dictatorships, but rather to paint a broader picture of living under surveillance. We recruited and interviewed ten participants overall, a relatively small group but revealing nonetheless about the practices of this difficult to reach group.

In our results we document what we call 'practices of surveillance'. There are four main areas that we focus on. The first one is about the agencies doing the surveillance itself (the 'surveillant') – in particular how the surveillance agencies were seen by our participants. We talk about how our participants needed to imagine and speculate what (and sometimes why) the surveillant was doing what they were doing, so as to react to that in their own practices. Sometimes ongoing investigations, or even arrests, put our participants in direct connection with these government agencies – confirming or changing their view of the imagined surveillant to a greater or lesser extent.

This leads us to discuss how our participants were dependent upon digital technologies, but also put in danger because of their use. This '*danger but dependency*' can be seen in social media use: they relied on it to publicise, recruit and advertise their activities, but also these actions made them vulnerable. This leads us to our third finding that emerged from the analysis: strategies of *enclosure or openness*. Different participants discussed how they used technology to protect themselves from the surveillants. Some tried to enclose different parts of their life, to build up a sort of "onion" of different rings and layers of protection. Alternatively, others tried to live a much more open life – what one participant called 'the open world' – where they assumed everything was visible by others and there is no point in trying to hide from them. This open strategy however comes with the cost of self-surveillance and even the surveillance of others, so as to not incriminate or put in danger oneself or others.

Our fourth point of analysis focuses on the effect of surveillance on *belonging to groups*. For many of our participants, their activities depended upon organising with, and mobilising others. Belonging to a group or a host organization had effect of exposing individuals to surveillance, since a group can be targeted or compromised. This led to the adoption of a "security culture" within groups with different methods and resources used for eluding surveillance, which we describe in our analysis.

Finally, we expand on what we can learn when it comes to thinking about the roles of digital technology in our lives. How do we 'design for the dissident' in HCI, and how can we deal with the difficult moral questions that this raises? We discuss how technical solutions become part of broader social practices that enable, hinder, protect but also expose those who are involved. We conclude by advocating for research that takes into account a critical view of the state in HCI and more broadly for an anti-surveillance stance in the design of technologies.

BACKGROUND

Dissident use of networked communication has been a recent focus of study in HCI, covering in a variety of settings, for example on protesting housing policies in US [2], supporting uprisings in Tunisia [47], political activism in Palestine [4,46] or guerrilla warfare in Colombia [9]. These studies highlight the thick connections between offline and online communication in order to support organizing while often having to avoid interference from state actors. HCI researchers also studied activism on more wide scales, such as the European anti-globalization movement [38], where large organizations sustain themselves by constant re-organization and through informal ways of transferring knowledge. Although this prior research also necessarily deals with surveillance, it differs from the research presented herein, as we do not focus on one particular cause, context or organization, but rather on the individual, long-term experiences of those living under state surveillance.

Surveillance has been broadly defined as processes of monitoring and record-keeping of individuals, ranging from making lists of personal details, to CCTV cameras [19]. These processes are increasingly embedded in everyday life and are often established to promote security, justice and participation in public life [27]. Mundane examples of surveillance are access cards in public buildings and biometric scanners in airports. There is a growing concern among scholars that many of these practices and technologies can unfairly impact different populations, lead to less choices and impact the quality of life of individuals [ibid]. In this paper we touch upon broader issues of surveillance, although our focus is on state surveillance, when directly focused on specific individuals.

Work on HCI around surveillance has mostly focused on privacy concerns, particularly in social media, which is understandable as these are issues concerning a wide population (e.g.[23]). A particularly relevant strand of research concerns interpersonal surveillance for communities or users with heightened secrecy needs. For example, Lingel *et al.* [25] examined how a music subculture engaged in organizing quasi-legal activities adopts specific security practices, using social media anonymously and subtle queues to distinguish between members and outsiders. Other researchers looked into particularly vulnerable communities. Freed *et al.* [14] have looked into how violence in intimate partnerships can manifest itself through adversarial use of common applications and services. Attackers have also harassed victims through revealing public information. Yarosh and Svetlana [48] have also examined how recovering addicts struggle with the use of technology in mediated group communication and social media, when anonymity concerns are central.

State Surveillance

If concern for interpersonal surveillance can cause anxiety for social media users, this concern can be exacerbated when it relates to more large-scale, organized and purposeful

actors, such as state security surveillance apparatuses. Shklovski and Kotamraju [41] found that state censorship affects how people change their technology practices: they self-censor themselves online, become more technically proficient in order to access blocked content, and practice radical openness and transparency in their everyday lives to show that they have nothing to hide. In another study where they look at both sides of surveillance, Shklovski *et al.* [43] show that surveillance technologies change relationships between parole officers, parolees and the communities where these are inserted, by placing the technologies in the centre of how parolees became accountable. Guberek *et al.* [17] studied undocumented immigrants' use of ICT, and found that they have a heightened awareness of state surveillance, consistent with their heightened vulnerability, but do not take added measures to protect their privacy. This is consistent with the phenomenon that researchers call "privacy paradox", which has been repeatedly observed in the general population [35]. This paradox postulates that individuals do not act on their expressed privacy concerns. Many reasons have been attributed for this paradox, namely that individuals have misconceptions of how information flows or are unaware of protective measures [ibid].

While the generalised aspects of state surveillance have been well discussed (following, in particular, revelations about the mass surveillance and storage of internet data [28]), surveillance also manifests itself on the level of specific groups and individuals. Some communities, such as journalists, have long-standing concerns with organized surveillance, namely to uphold high-regarded professional standards such as protecting sources. McGregor [31] studied how diverse and often conflicting these measures can be. Journalists often rely on ad-hoc negotiated security practices, between themselves and the sources and between colleagues, rather than unified or "proven" security practices. This lack of unification makes it difficult to design security tools to fit all types of methods. Indeed, the lack of technical savvy means that some journalists may not be protecting themselves or their sources [ibid].

Like journalists, activist organizations are also a usual target of state surveillance. Recent work on the practices of activist networks [26] has found that activists fight to become visible and to publicise their cause, adopting varying strategies of radical transparency to both protect themselves and project their message. A related technique is to use 'reverse surveillance' to map state players, and those involved in surveillance, tracking those who are trying to track them.

State surveillance is often portrayed as an activity mainly concerned with data collection. However, it is also important to understand the activities that often go hand in hand with collection. For example, some scholars have started to warn of concerted efforts by states to exert control over all spheres of mediated life [29]. This "culture of control" [15] results in more than just tapping into communications, but also involves information censorship, personal harassment, releasing of personal information (similar to "doxing"), or denial of service attacks. Surveillance can then be understood as part of a politics of information control, specifically aimed at diminishing capacity of individuals and of organizations deemed problematic by the state.

METHODS

We recruited ten participants using a snowball sampling method [20], starting with personal contacts and also by emailing diverse non-governmental organizations. Five of our participants are activists and have been arrested or interrogated by police or other state security forces, of which two are part of international leftwing anti-fascist networks, 1 belongs to an environmental organization, one works for a human rights protection organization, and one is a LGBTQ activist. Three were journalists reporting on issues considered forbidden by the states they worked on, but also independently blogged online. Two were gray activity workers (one was an organizer of unlicensed events), and their activities often put them in contact with police forces. Our participants lived mainly in European countries, and some in Asian countries. Since some of our participants have public visibility, to protect their anonymity we refrain from providing biographical details on each.

Looking at surveillance from the point of view of those under the eye of law enforcement, a group generally neglected in HCI, gives us a coherent sample to discuss wider issues in surveillance in society and the role of HCI in it. Our criteria for participation was to self-reportedly have obtained proof of having been under surveillance by security forces, either through transcripts of their own communications, or having been detained in connection with monitored communications.

As one could expect, this is not a particularly easy group to contact; we relied mostly on personal connections for the recruitment, and did not make any public announcements concerning the research, beyond a webpage on our university webserver, as proof of our affiliation, that we made available to participants outlining the study and our goals. Along with explaining our research goals at length, and offering our participants the opportunity to remove themselves from the study at any point, our participants signed a consent form, in which they gave us permission to publish academic work directly quoting from the recorded interviews or notes. Although we provided no financial compensation for participation in the study, we shared information and technical expertise whenever possible, after the interviews were conducted. Some of our participants may be at risk, which is why we abstain from providing identifiable information or ascribing individual quotes.

Along with personal contacts, some of the initial recruitment was done through email by directly contacting well-known activist or media organizations. We explicitly tried to recruit a diverse sample and our initial contacts had no connection with each other, but also engaged in very different activities. As is typical with a snowball sample [20] we asked our initial participants to recruit further participants from their

acquaintances. Often, the people who we initially contacted declined or did not qualify to participate in the study and referred instead others. Snowball samples are particularly appropriate for hard to reach groups, and where exposure of membership in that group is potentially threatening. Using this method we cannot speak to the representativeness of our participants, but this is outweighed by the value of reporting from an otherwise neglected social group [ibid].

We took extensive steps to protect the anonymity of the participants – including keeping records of the interviewees and analysis offline, in a physically secure location, as we developed our analysis. The interviews were done in accordance to the participants' wishes, in their own language if possible, and respecting their security concerns. Due to the wide geographical distribution of our participants, some interviews were done remotely. As such, 4 interviews were done in person and recorded, 4 were done through an encrypted audio calling service and recorded – except for one, for which we only took notes, and 2 interviews were done through textual encrypted messaging service. Interviews done in person or through audio call lasted between 40 and 75 minutes. Most of our interviews were recorded (and kept on offline storage). Some interviews were only partially recorded, as our interviewees often asked to go off-the-record in order to approach particularly sensitive subjects or security practices that they did not want to be known. If particularly sensitive data made it into recording, we erased parts of this record. For audio interviews, we have transcribed them ourselves. We circulated pseudonymized transcribed quotes during analysis and drafting of the paper. In the final version of the manuscript, we took a step further from pseudonymizing quotes by grouping interview subjects and labelling each group by the activity that qualified them for this study – activists, journalists and those working in gray or illegal activities. This provided a reasonable balance between anonymity and contextualization of the data.

Analysing Interviews

Interviews were transcribed and translated to English whenever applicable. A thematic analysis was then conducted on the transcriptions. Our goal in the interviews was to understand different pressures and practices, with as broad a perspective as possible. We were not looking for statistically generalizable points, but rather generating concepts and understandings of our participants' practices, emotions, actions and reactions. As such, our approach to analysing the interviews drew on an interpretivist stance. The analysis involved open coding of the interviews, and the development of themes through an iterative process of concept development.

We sought to cover a wide range of activities and actions, different organizations and countries, spanning two continents. This study has therefore an important limitation in that we are not able to go into specifics about how particular security forces conduct their work or how particular organizations or individuals conduct activist practices. Our study can only illuminate some broad common themes about experiences and practices of living under state surveillance.

Ethics

As already mentioned, we have taken precautions for anonymization and censoring of data. Additionally, following best practices around research with sensitive individuals in HCI [41] we have chosen not to identify the countries where our participants come from, not to disclose any organizations, and to withhold any information that we believe may lead to identifying our participants in this manuscript, as it has the potential to cause harm to them or their families.

We also wish to disclose that the authors are also involved in the communities that they recruited from, although very marginally. This made it possible to do some of the recruitment. Additionally, we explicitly do not distance ourselves from the dissidents we portray here. In fact, we defend that most people in some way or another have encountered systems of oppression which they resisted, many have conducted civil disobedience actions, and most people have committed activities that can be considered to be criminal (e.g. 32% of US citizens and 45% of EU citizens admit to have acquired and consumed pirated media content [52]). Our position is that we assert the right to dissent, or to object to established laws and regulations. We are also not opposed to the existence and activities of security forces, including surveillance. Our conception of surveillance is that it is a complex practice and should be treated as such.

ANALYSIS

Our analysis focuses on four broad themes: how participants conceive of or imagine those monitoring them: *the imagined surveillant*; their relationship with ICT: *danger and dependency*; strategies to cope with state surveillance: *enclosure and openness*, and how *belonging to a group* of dissidents can both protect from and heighten vulnerability to state surveillance.

The (Imagined) Surveillant

> **Surveillant.** *Noun:* a person who exercises surveillance [53]

State surveillance relies upon a fundamental lack of symmetry – those under surveillance often have little definitive knowledge about how and when they are being monitored. This meant that our participants, to a large extent, had to *imagine* the agencies monitoring them, who they are, their motivations, and how they operate. These were "folk theories" of a sort [16], constructed by piecing together incomplete information, but they illuminate how each participant conceived of the security forces, and how they attempted to mirror how they believe agencies were monitoring them.

All our participants identified the government or security forces working for the government (mainly police forces) as their main surveillant. Yet, as one participant put it, the ones who should be blamed are the lawmakers, who set the laws and decide what should be forbidden and what should not,

and not the police who are just following instructions from the lawmakers. All our participants did not blame low ranked security forces for surveillance and harassment. Instead, as one of our participants mentioned, there is a perception of a system, christened by one of our participants as a "*republic of stupidity*" where agencies justify their budget by collecting often unnecessary data on people, who are put under surveillance for opaque reasons. These reasons were usually described as strongly politically motivated, in order to dissuade or curb protests, particularly those deemed to be more disruptive to political meetings such as climate conferences and G20s, or during election periods. As one participant put it, surveillants are generally interested in anybody who is against "*the democratic nature of the state*", describing the 'problem' as people being either extreme left (anarchists) or extreme right (fascists). The goal of surveillance for the police and consequently the government is to protect the status quo:

> "*In general the police is here to protect the status quo and everything that is a bit outside of that, they're here to stop that*" (Gray/Illegal Activity Worker)

This said, some participants talked about how surveillance is connected to deeper values of democracy, including who defines what civil disobedience is. One argument was that civil disobedience should be performed openly and it should be a living discussion for everyone, questioning society, and consequently the boundaries of democracy. As one participant described it, fighting for environmental issues required demonstrating against the operation of power plants – something considered by the government as a form of eco-terrorism:

> "*Some political parties, some people from the liberals - legal spokesperson- went out clearly and said: "Look at what's been done, we should include eco-terrorism into the secret service of [country] into what they should surveil". […] It's a crucial debate for us, to defend civil disobedience*" (Activist)

While most of the 'folk theories' that our participants presented cannot be substantiated by definitive proof, all of our participants reported obtaining concrete proof of being personally surveilled or being implicated in surveillance done on close associates at some point. Security forces can make their presence deliberately or unwittingly known, such as police taking photos of protestors during demonstrations, or, in one case, security forces sitting outside their apartment making no effort to conceal themselves:

> "*Sometimes there are cars, there used to be some cars of government. Mostly occupied by security people, waiting at our door specially a year and half ago*" (Activist)

Another participant shared an incident of being actively monitored by police. As they described it, a van with police officers was waiting outside their apartment, one day after a protest in which they participated. When the participant saw them and ran away, the police started chasing them until they lost them. However, since this was only one incident, the participant had no concrete evidence of whether and when surveillance was happening.

Other than seeing the security forces possibly carrying out the surveillance, there are more concrete signs. One comes from having transcripts of private conversations, digital trials, and surveillance photos presented to them during an interview with the state apparatus. Three of our participants mentioned being explicitly shown printed evidence of personal online messenger conversations, as evidence of them being under surveillance. One of these participants discussed how the police, in country where they went to investigate a political murder as a journalist, casually revealed private information in a conversation that could only have been obtained through monitoring. Similarly, another participant was shown evidence of registered private conversations through mobile phones:

> "*In [country] we were being tapped […] and then also taken into custody because they [police] have tapped mobile phones. We got the manuscripts of the conversations*" (Activist)

Additionally, as part of surveillance efforts, security forces may make themselves visible by arresting and interrogating friends, family or co-workers about them, or visiting their workplaces or homes unannounced. This is seen by our participants as unwarranted harassment:

> "*During those days one of my sisters was interrogated unofficially and against the law. They don't go to law to get the interrogation warrant, to scare people. To scare a pregnant woman and her kids, they take her to the security room with someone you wouldn't know who s/he is, of course she will be scared and this will mess with her life*." (Journalist)

Indeed, it seems that this was an important role of surveillance – not to gain information by the state but as a form of harassment. The constant pressure enacted by being under surveillance could cause individuals to abandon their at risk activities – or simply the surveillance itself could act as a punishment of sorts.

This said, an absence of evidence could not be reliably taken as evidence that one was *not* under surveillance:

> "*Since I have certain phone numbers and connections with some people, I would always suspect that my phone is tapped. That doesn't mean that someone will actively listen to my calls, but basically that they'll put messages and GPS data somewhere on a server and have access to it, if they need it*" (Activist)

As many of our participants are mobile and travel overseas, we observed that they believed security agencies in different countries had different capabilities and objectives. Some considered the police to be monitoring in some countries where their organization operates but not in others and felt

safe in countries where they perceived police to not be specifically targeting them. One participant had moved abroad as they did not feel secure in their home country, mentioning that it is harder for one state to get personal information from another state, when living in another country:

> "*In case of [country], they don't have access to this [personal] data of us living abroad, not that they don't want to use it against us, they just don't have access to be able to use it*" (Journalist)

Clearly, the understanding of how surveillance works for our participants is of a patchy and highly politicized system, where interests of political parties, competing governments, and international interests are mobilized for surveillance in different times for specific purposes.

Danger and Dependency

As ICT pervades more and more aspects of our everyday lives, digital trails are increasingly left behind by every transaction and communication act. All our participants are acutely aware of this. Below we elaborate on two aspects related to danger and dependency emerging from our interviews, namely the need for real world interactions, including communication with family and loved ones, and the need of social media for organizing acts, and how these practices can be monitored.

All our participants believe that data posted in digital forums such as social media or digital/wired communication channels could be potentially tapped by a state actor with an interest in them. Yet participants were also dependent upon using social media and electronic communication more broadly. The actual activities that caused them to be under surveillance– e.g. organising illegal parties – often relied upon using social media in some way. Another example includes the need to mobilize others, e.g. for activist actions, it makes sense to have a public facing profile in social media. Activists often have some public personal profile primarily maintained for online communication. The 'fame' of the dissident, for example, comes from having some sort of presence in a community, one that can be established by face to face contact, but also online.

Sometimes there was a specific and more direct need for online communication and social media. One participant who arranged illegal parties talked about how the location of an event might be released at the last minute so that the police will not have time to organize themselves beforehand and stop it. Social media was therefore required to both publicise the event but also to control attendance – with those signing up online getting their names printed so that they could get tickets later. Clearly, while the online created very clear and present dangers, they were also very dependent on it. Alternatively, another participant discussed how they did *not* make use of secure communication apps, reasoning that having a particularly 'hardened' software like Signal would mark them out if they were searched. Accordingly, they made use of everyday messaging software that used encryption as default (such as WhatsApp).

Surveillant agencies can get access to online data by using a range of means, for example through backdoors, hacking, official judicial access, direct wiretapping, or by impersonating friends, having access to friend-facing social media profiles and communication. Often those under surveillance are not sure of the exact ways that they are being surveyed online:

> "*We are under pressure and surveillance from [country]. My account was hacked, maybe downloading something or opening a wrong link, I don't know for how long it's been hacked, [my organization] security team got involved and I got my account back*" (Journalist)

One central aspect to everyday life is personal communication at a distance, either with family members, friends or other fellow activists. Some communication can be avoided, like avoiding talking to their family over networked channels but often the organization of an action, such as a protest, requires communication to take place. Some participants talked about selective use of social media channels as a way to tackle the contradicting nature of danger and dependency, especially since "*it is very difficult to live completely without technology, and this takes a lot of effort.*" (Activist). Depending on the threat model, some channels were preferred to others, for example encrypted channels to non-encrypted ones are often preferable:

> "*If we want to plan a protest or action, we usually communicate through encrypted text messages, or some other collaborative platforms that exist, but it's hard. There are many in person meetings also*" (Activist)

Many aspects of how our participants live out their activism, as well as everyday lives, intersect and depend on ICT, making every technology mediated aspect of life a danger, as well as a (often inescapable) dependency. This aspect is obvious in online communications and online appearance in social networks, which are increasingly crucial to organize protests and actions. But at the same time, digital trails are increasingly left in many other, also crucial aspects of everyday life and organization, such as financial transactions, face-to-face communications, walking in the sidewalks of a camera-monitored street or even using public transportation, as well as traveling overseas. Mobility is also monitored, as for example international mobility is well-known to be a site of inspection, particularly when applying for visas, or when travelling to specific countries. Cameras, logs of using transportation cards for public transport, GPS trails, are all considered by our participants to be stored in servers and be ready to be accessed by security forces should they need. This highlights the everyday life dependency of need for mobility in city either using streets or transportation, or the need to use financial transactions in order to sustain life, and the increasing data trails left in all aspects of life. One

participant had been trying to be completely "invisible" from society and the state system for the past six years: "*I don't have a bank account or any other thing in my name. […] I hardly exist on the past 6 years*" (Gray/Illegal Activity Worker).

Enclosure and Openness

The dependency on and pervasiveness of technology in everyday life, knowing that every personal detail can be potentially tapped gives rise to different strategies to cope with it. All our participants live with the assumption that communications can potentially be watched – but also that they could never predict when they were no longer under surveillance. As one participant put it, *once under surveillance, always under surveillance*.

One way of dealing with this was a strategy of *enclosure*, when our participants choose to limit their visibility to the world. This sometimes translated into avoiding the use of social media:

> "*I generally don't use social media, and it's not something I miss. But even owning a computer and especially a smart phone is a huge security risk. So that is a compromise in its own right. I try to be careful with that and it's important to know when to turn it off*" (Activist)

Another participant talked about their practice of deactivating their twitter account a month before every trip to US, since "*any twit that I post then may cause a problem for my next business trip. A month before every trip to US I deactivate my twitter account.*" (Activist) As surfaced by the interviews, limiting sharing of public information to certain times is also an important enclosure practice to deal with the danger of using social media. Our participants often choose to avoid certain topics in mediated communication channels, such as avoiding topics seen as sensitive:

> "*We know they are listening… this stress is always there but we try to not get into this conversation [about being listened to on the phone]. We try to not talk about it, about this kind of topics that may tickle them, like political topics, country related* " (Journalist)

Besides avoiding topics in mediated communication, some participants also censored who they interact with. This can be done by heavily curating social media profiles or abstaining from social media entirely, to avoiding making new friends in real life. This is based on the belief that abstaining from social exposure can help protect the people around them as well as themselves, as they do not necessarily trust new people who try to be their friends. Some of our participants went to lengths as to try to moderate how their acquaintances (friends, family) shared content on social media or other channels.

> "*I had to cut with some of my friends because I cannot be sure this photo they are taking from me today will be used tomorrow for what exactly*" (Activist)

Enclosure could work on different levels – rather like the classic model of the onion, with different levels of security for different people, with different barriers set up between the different groups.

Another set of practices can be grouped around the theme of *openness*. Different participants talked about taking an approach of enclosure or openness, but at times participants also mixed these approaches. Openness was based around having nothing to hide with regards to activism and social connections. As one of our participants puts it, "*the more private and secret something pretends to be, the less people trust it*" (Gray/Illegal Activity Worker). In fact, being open can also, personally, be part of a strategy for dealing with the fact that they can be exposed at any moment. As one participant put it, being open can be part of a "shield", so that security forces cannot use their activism against them in personal and professional parts of their life.

> "*I have the antifascist t-shirt that I wear at work, in that way I feel that I don't hide anything, I am who I am. Some people think this is provocative but I would rather have that, or the opposite would be that the police comes to my work and they ask to talk to me and my boss […] and I would stand there with my T-shirt. That is a coping strategy, to be proactive. It is a way to "normalize" it, beforehand*" (Activist)

Another participant discussed how everything that they do in private has to be defensible in public in any situation, due to their previous experience of private communication being shown publicly:

> "*It is obvious to me that when it comes to political topics, I cannot hide anything for a long time. […] This is about public concerns, meaning that in private I would talk about political views that I can defend that view in public too. This is to always be ready for that private conversation [topic] to become public*" (Journalist)

In general, our participants have a heightened awareness of how data from everyday infrastructures can be mobilized and aggregated by security forces, suffering from function creep [1], making it impossible to uphold the notion of contextual integrity [33]. Paradoxically, "being open" on a personal level can be achieved by deliberately breaking barriers between different personas (e.g. the dissident and the family person) and by actively censoring topics and hiding aspects of personality. What is left in the "open", for most of our participants, is in fact a carefully curated persona. This anti-surveillance tactic of openness has been found in other research on dissidents [26,42].

Belonging to a Group

Some of our participants perform their main activities in groups (e.g. organizing protests), while others work mainly alone (e.g. bloggers). Although all depend on others to live their lives, there are some aspects specific to belonging to a group that surveillance disrupts. For example, organizations

doing some forms of environmental activism such as boycotting power stations can be classified by a government as "eco-terrorism" and therefore warrant surveillance under anti-terror laws. Participants can also be marked for surveillance by associating with known organizations or with individuals who are assumed to be under probable surveillance. Being part of a group then is both seen as enabling action and impact, but also posing additional risks. Being part of an organization can grant some protection from surveillance. Formal organizations have IT security teams, physical security teams, and legal experts that make sure that members communicate securely with each other and can be protected and even repatriated in case they get into confrontation with security forces. More informal organizations also have concerns with setting "security culture", where members protect each other.

> "*I think it is quite easy to set up a good security culture where people can understand and evaluate risks. […] new people or people that are at least new to participating in actions sometimes as simple as a rally often don't grasp the amount of risk they are involved in*" (Activist)

Sometimes, specific aspects of mediated communication for groups make it preferable to face-to-face contacts. ICT can enable connecting with strangers to gather people to events, communicating with groups where participants can participate semi-anonymously. Interestingly, although most of our participants make use of one or several encrypted channels for mediated communication, none of them really trusted encryption as a sole measure of security. When asked why, reasons varied from not being technically competent enough to be sure that the communication is secure, to having a strong technical background but assuming that all encryption can be broken in the future:

> "*Those are kind of superficial precautions. Even encryption. Basically, it would take them now a month to decrypt a PGP mail*[1]*. But in a few years, maybe a few months even this amount of time will come down to minutes just by a brute force try*" (Activist)

Encryption appears, rather than being a silver-bullet solution, is instead used as part of a wider set of practices that aim at protecting identity of groups. Rather than relying on technical means for communication, these security practices rely on ways of organizing. Nearly all our participants shared with us some sort of favourite method that they had for eluding surveillance. We called these practices 'magic methods' – since while they were all different and seldom there was any evidence to their efficacy, they were introduced to us as a sort of shared secret – a magic way of escaping from the ever present gaze. There was a range of different 'magic methods' that we were introduced to – some for establishing trust between members of an anonymous group, enabling members to have plausible deniability of group membership, sharing limited information when needed (e.g. location for events being shared in the last minute so that security forces could not prepare in advance), or group practices for dissolving and re-assembling groups whenever the group has been compromised or infiltrated. For example, one of our participants shared that they would give their social media passwords to a trusted person to remove their own access to their accounts in case they were interrogated. Another participant had a method to create groups anonymously using Twitter:

> "*We made a group and everyone in that group made an alias and created a twitter account joining that group with a dedicated sim card. One in the group is assigned as the trustee who had all information, knew which individual is behind which account but wouldn't share it with others. This way everyone knew who is the trustee, but they didn't know each other in the group*" (Journalist)

Assembling groups anonymously was important, but so was re-assembling the group whenever someone or some device got compromised, as exemplified by another method shared by this participant:

> "*We use group chats with many people involved, and once someone's phone got snatched, so everybody had to leave this group chat, and we had to create a new one. And then two other people who came with the ferry got snatched, so we had to create a new group again*" (Activist)

The same participant also said that it was a normal practice to carry a second phone to protests that has less accounts and contacts in it, with "*low surface area*" of personal information about themselves and others associated with them. While these methods could of course be effective, it is the nature of being under surveillance that the end user can never know for sure. This lack of knowledge of course added a level of ritual to these practices, which they were not done for evidential reasons but because they had apparently been effective in the past.

DISCUSSION

These four sections give some insight into the practices of those under surveillance. Much of what our participants did was inherently under considerable ambiguity – with a need to react and plan with respect to an 'imagined' surveillant. Yet clearly serious issues were under question– many of our participants had had their liberty threatened. Our participants were both dependent upon communication technology, but at risk because of it. This led them to adopt a variety of different resistance practices – from trying to be open and having nothing to hide, to carefully enclosing their life and social contacts in different layers. For our discussion we engage with these issues in three ways.

[1] Pretty Good Privacy (PGP) is a technology originally developed for encrypting email communications [49]

First, we explore how could we design for the dissident, focusing on two aspects. Our participants had to continually adopt and reassemble their technical setup and practices to protect themselves. This would suggest then that there will not be one app or solution that can counter the power of the state; rather an ever-changing bricolage of different tools and solutions. On the other hand, dissidents are seldomly acting alone. Discussions around surveillance tend to focus only on individual protectionism of information through, for example, cryptography and anonymization. But our study also suggests that there is a need for supporting plausible deniability and ways of controlling facets of identity.

As we mentioned in the introduction, our goal here is to spark critical reflection on the way our technologies are being used. The second section addresses the important question "whose side are we on?" While we might want to remain neutral to some extent, and certainly there are no easy moral positions, we would argue that the increasing ease of mass surveillance makes an important argument for technologists, HCI included, to urgently work to find ways of making visible the predominant power of the state. This leads us to our final discussion point where we argue for a more skeptical view about the benevolence of the state in HCI.

Designing for the Dissident(s)

The untrustworthiness of technology was perhaps the most ever-present comment in our interviews – it was something that had to be relied upon but could never be trusted. Clearly there is likely not one technology or platform that will be safe from state surveillance in the long run. From our participants perspective, eventually every technology would be circumvented, every system had a shortcoming, encryption could be broken, and communication devices turned into surveillance devices. Indeed, this expectation does not seem unreasonable - recent news reports have revealed how both iOS and Android phones have suffered from so called '0-day' vulnerabilities, and that by simply visiting a particular URL could result in tracking software embedded on your device [54].

Our participants talked about constantly moving and changing their setup - moving from one communication software to another, one social media platform to another, resetting devices or maintaining multiple devices for different settings. As participants used devices and services over time they would collect the 'patina' [13] of their past activities and contacts, and eventually these would have to be wiped. If this untrustworthiness is an unavoidable feature of technology, one point for discussion is how to *design for an untrustworthy system.* More importantly, we advocate designing information and communication technology that balances the need to connect with the need to be invisible. Our participants needed 'plausible deniability' – for example, we have shown how being part of a group is both a source of vulnerability but also enables actions and anti-surveillance practices. Additionally, when belonging to a group, dissidents rely on each other to keep compromised members (when arrested and interrogated for example) or compromised devices (hacked or apprehended) from compromising the rest of the group.

Plausible deniability by design would allow dissidents to deny belonging to groups, distancing themselves from actions of others or actions executed by themselves in the past. So called, ephemeral messaging apps, such as Snapchat already support disappearing messages, but plausible deniability by design could extend to other technologies, allowing for deniability of having specific contacts, denying posts on social media, or even having certain apps on their phones. Ephemerality here – such as deleting contacts, photos or even apps after a few days could help. How could we design platforms that support generation of fluid groups, supporting ephemeral associations between dissidents, with just enough information sharing to e.g. plan a protest? We note that in the recent (2019) protests in Hong Kong, protestors have adopted the messaging software 'Telegram' not because of its use of encryption but because it reliably deletes messages, and allows communication amongst anonymous groups [51].

Building on this, we advocate designing not only for anonymity but instead for how to *keep different facets of identity separated from each other in online communications*. There are cases when dissidents might wish to stay anonymous but often there is a related need to maintain a public persona. However, we have seen how state surveillance also impacts how our participants relate to their friends, families, and other dissidents. When using technologies, dissidents adopt different tactics, either layering different levels of information sharing for different people, or radically being open due to inability of keeping their dissident personas hidden. Although in most online platforms it is possible to do so by using different nicknames or email accounts, it is not always easy to separate different facets of ourselves. A commitment for *identity management* online, in the hands of the users, could inform design decisions in technologies for example by not requiring real names to be provided, such as the case now in Facebook, or more broadly as an argument for right to control different facets of one's online identity in search engines [7].

Whose Side are we on?

In 1964 the sociologist Howard Becker asked of social scientists: "Whose side are we on?" [3], questioning the neutrality that social science often adopted on the major social issues of those times. This is a question we have grappled with in this work, and one that is increasingly causing difficulties in HCI research that discusses seriously the implications of controversial work. The adaptability of technology means that a system designed for activists can in turn be used by paedophiles; surveillance technology is used by democracies and dictatorships alike. Is it then possible for us to 'take a side'?

As been long established in science and technology studies, technologies are themselves not neutral; they are created in

particular contexts and designed and put to particular uses. For example, nearly all those employed in cryptography in the US are employed by the state, with research directed towards supporting surveillance in some way or other, rather than preserving individual privacy [37]. Yet the question of whether the surveillance of the people we chose to interview is warranted perhaps depends on the who is making that judgment. Many will feel that political opinions *should* be controlled, or that cannabis should not be planted, that all music events should have permits, or that environmental protests should be curbed, and feel that actions of security forces are justified so as to balance other values like public safety. These are fundamental differences of opinion.

It is clear that universal and standard ethical codes of conduct are not sufficient, since we will not be able to predict how the design choices we make will generate future possibilities and unknown consequences in different contexts [30]. Our proposal is therefore to notice the practices and livelihoods of those under the eye of security forces and consider them when approaching tech design. We choose to take their side, by advocating for adversarial research in HCI [11] supportive of dissent, or engage in undesigning practices [36], challenging wider societal practices with clear aims of inhibiting and foreclosing technological possibility for data accumulation and function creep.

The State and HCI

While recent critical debate around technology has rightfully addressed issues of data capture by private companies, the state is also of course a willing and active agent here too. The state is a powerful actor in all our lives, as well as in our use of technology. In HCI, while the state has been critically examined in the 'digital civics' programs [10,21,45], broadly the state is still described in benevolent terms. Digital civics [34] aims to empower citizens through the use of digital technologies, collaboratively working with states to produce "*alternative models of service provision*". While this is a critical engagement, what our participants had to deal with was something perhaps rather more hard-edged - the state as a bad actor, not only in opposition to their goals, but also threatening their existence.

From a democratic perspective we are perhaps used to seeing the state as a benevolent agent, respecting the rule of law. But for our participants, who also mainly live in democratic societies, the state actively threatened their lives. Any comprehensive consideration of the state then needs to move beyond an assumption of benevolence. Moreover, it is not unreasonable to assume that many parts of the state act as if they are not bounded by law. They exist through extreme interpretations of law that bureaucracy manages to protect from proper scrutiny. While we would not – and our participants certainly did not – argue that 'all states are the same', even the most benevolent states have elements of them that could be properly described as bad actors. Our point is that *all* states have negative and harmful elements.

Learning from the practices of those in the margins could help us take a much more critical view of the state in the ways in which it manifests itself. It seems to us that the bureaucratic and at times threatening nature of the state has been somewhat neglected in HCI research. Building on this, we see value with engaging, not only with "illegitimate" forms of political participation [2], but also with groups that live under constant threat of the state, such as undocumented immigrants [18]. Treating the state as a non-benevolent actor can have implications for the design of activist platforms by considering a broader range of relationships between citizens [22] and between citizens and state, and perhaps even contribute to make some forms of illegal dissidence more legitimate.

CONCLUSION

In this study we have engaged with a difficult, and controversial topic. Through inspecting the practices of those who are 'under probable surveillance' we have tried to understand both the role of technology, but also the broader social implications for our participants of prompting the unwelcome attention of the state. We would imagine that there will be many who will disagree with our views. There are also many shortcomings in our work here. We deliberately chose only to interview those under probable surveillance, and to not include those who conduct surveillance themselves. This is balanced with the opportunity here to document the experiences of a group that is seldom engaged with within HCI.

In the discussion we used their practices as a way of engaging with the question of how (or even if) we should be designing technology that circumvents or protects itself against surveillance. With the predominance of power – both political but also in terms of technical development – on the side of states we advocate for research focused on countering the current expansion of surveillance in our societies, and a critical view of the role of the state in HCI.

ACKNOWLEDGMENTS

First and foremost, we thank our participants. We would also like to thank Kristina Höök and Donny McMillan for commenting on early versions of this manuscript. This work has been partly supported by the Knut and Alice Wallenberg Foundation (KAW) within the project "Engineering the Interconnected Society: Information, Control, Interaction", Swedish Foundation for Strategic Research project RIT15-0046 and Swedish Research Council project 2017-04804.

REFERENCES

[1] Mark Andrejevic and Mark Burdon. 2015. Defining the sensor society. *Telev. New Media* 16, 1 (2015), 19–36.

[2] Mariam Asad and Christopher A. Le Dantec. 2015. Illegitimate Civic Participation: Supporting Community Activists on the Ground. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (CSCW '15),

ACM, New York, NY, USA, 1694–1703. DOI:https://doi.org/10.1145/2675133.2675156

[3] Howard S. Becker. 1967. Whose Side Are We On? *Soc. Probl.* 14, 3 (1967), 239–247. DOI:https://doi.org/10.2307/799147

[4] Nina Boulus-Rødje and Pernille Bjørn. 2019. Digital (Occupied) Palestine. Retrieved August 20, 2019 from https://forskning.ruc.dk/en/publications/digital-occupied-palestine

[5] Simone Browne. 2015. *Dark Matters: On the Surveillance of Blackness*. Duke University Press.

[6] Monika Buscher, Markus Bylund, Pedro Sanches, Leonardo Ramirez, and Lisa Wood. 2013. A New Manhattan Project? Interoperability and Ethics in Emergency Response Systems of Systems. In *10th International ISCRAM Conference*.

[7] Markus Bylund, Jussi Karlgren, Fredrik Olsson, Pedro Sanches, and Carl-Henrik Arvidsson. 2008. Mirroring your web presence. In *Proceedings of the 2008 ACM workshop on Search in social media*, ACM, 87–90.

[8] Baki Cakici and Pedro Sanches. 2014. Detecting the Visible: The Discursive Construction of Health Threats in a Syndromic Surveillance System Design. *Societies* 4, 3 (July 2014), 399–413. DOI:https://doi.org/10.3390/soc4030399

[9] Débora de Castro Leal, Max Krüger, Kaoru Misaki, David Randall, and Volker Wulf. 2019. Guerilla Warfare and the Use of New (and Some Old) Technology. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, ACM Press, New York, New York, USA, 1–12. DOI:https://doi.org/10.1145/3290605.3300810

[10] Eric Corbett and Christopher Le Dantec. 2019. Towards a Design Framework for Trust in Digital Civics. In *Proceedings of the 2019 on Designing Interactive Systems Conference* (DIS '19), ACM, New York, NY, USA, 1145–1156. DOI:https://doi.org/10.1145/3322276.3322296

[11] Carl DiSalvo. 2012. Adversarial Design as Inquiry and Practice. In *Adversarial Design*. MITP, 115–125. Retrieved December 18, 2019 from https://ieeexplore.ieee.org/document/7159941

[12] Virginia Eubanks. 2018. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Publishing Group.

[13] Pedro Ferreira, Pedro Sanches, and Alexandra Weilenmann. 2013. Awareness, Transience and Temporality: Design Opportunities from Rah Island. In *Human-Computer Interaction – INTERACT 2013* (Lecture Notes in Computer Science), Springer Berlin Heidelberg, 696–713.

[14] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. A Stalker's Paradise. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, ACM Press, New York, New York, USA, 1–13. DOI:https://doi.org/10.1145/3173574.3174241

[15] David Garland. 2002. *The Culture of Control: Crime and Social Order in Contemporary Society* (1 edition ed.). University of Chicago Press, Chicago.

[16] Susan A. Gelman and Cristine H. Legare. 2011. Concepts and Folk Theories. *Annu. Rev. Anthropol.* 40, 1 (2011), 379–398. DOI:https://doi.org/10.1146/annurev-anthro-081309-145822

[17] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile? In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, ACM Press, New York, New York, USA, 1–15. DOI:https://doi.org/10.1145/3173574.3173688

[18] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H. Mhaidli, Kentaro Toyama, and Florian Schaub. 2018. Keeping a Low Profile? In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, ACM Press, New York, New York, USA, 1–15. DOI:https://doi.org/10.1145/3173574.3173688

[19] Kevin D. Haggerty and Richard V. Ericson. 2000. The surveillant assemblage. *Br. J. Sociol.* 51, 4 (2000), 605–622. DOI:https://doi.org/10.1080/00071310020015280

[20] Douglas D. Heckathorn. 1997. Respondent-Driven Sampling: A New Approach to the Study of Hidden Populations. *Soc. Probl.* 44, 2 (1997), 174–199. DOI:https://doi.org/10.2307/3096941

[21] Tom Jenkins, Christopher A. Le Dantec, Carl DiSalvo, Thomas Lodato, and Mariam Asad. 2016. Object-Oriented Publics. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), ACM, New York, NY, USA, 827–839. DOI:https://doi.org/10.1145/2858036.2858565

[22] Os Keyes, Josephine Hoy, and Margaret Drouhard. 2019. Human-Computer Insurrection: Notes on an Anarchist HCI. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (CHI '19), ACM, New York, NY, USA, 339:1–339:13. DOI:https://doi.org/10.1145/3290605.3300569

[23] Airi Lampinen, Vilma Lehtinen, Asko Lehmuskallio, and Sakari Tamminen. 2011. We're in it together. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, ACM Press, New York, New York, USA, 3217. DOI:https://doi.org/10.1145/1978942.1979420

[24] Marvin Landwehr, Alan Borning, and Volker Wulf. 2019. The High Cost of Free Services: Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure. In *Proceedings of the Fifth Workshop on Computing Within Limits* (LIMITS '19), ACM, New York, NY, USA, 3:1–3:10. DOI:https://doi.org/10.1145/3338103.3338106

[25] Jessica Lingel, Aaron Trammell, Joe Sanchez, and Mor Naaman. 2012. Practices of Information and Secrecy in a Punk Rock Subculture. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work* (CSCW '12), ACM, New York, NY, USA, 157–166. DOI:https://doi.org/10.1145/2145204.2145230

[26] Tetyana Lokot. 2018. Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices. *Surveill. Soc.* 16, 3 (October 2018), 332–346. DOI:https://doi.org/10.24908/ss.v16i3.6967

[27] David Lyon. 2010. Surveillance, Power and Everyday Life. In *Emerging Digital Spaces in Contemporary Society: Properties of Technology*, Phillip Kalantzis-Cope and Karim Gherab-Martín (eds.). Palgrave Macmillan UK, London, 107–120. DOI:https://doi.org/10.1057/9780230299047_18

[28] David Lyon. 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data Soc.* 1, 2 (July 2014), 2053951714541861. DOI:https://doi.org/10.1177/2053951714541861

[29] Rebecca MacKinnon. 2012. *Consent of the Networked: The Worldwide Struggle For Internet Freedom* (1 edition ed.). Basic Books, New York.

[30] Annette N. Markham and Princess Bride. 2006. Ethic as method, method as ethic. *J. Inf. Ethics* 15, 2 (2006), 37–54.

[31] Susan E. McGregor, Franziska Roesner, and Kelly Caine. 2016. Individual versus Organizational Computer Security and Privacy Concerns in Journalism. *Proc. Priv. Enhancing Technol.* 2016, 4 (October 2016), 418–435. DOI:https://doi.org/10.1515/popets-2016-0048

[32] Anthony Bolton Newkirk. 2010. The Rise of the Fusion-Intelligence Complex: A critique of political surveillance after 9/11. *Surveill. Soc.* 8, 1 (July 2010), 43–60. DOI:https://doi.org/10.24908/ss.v8i1.3473

[33] Helen Nissenbaum. 2009. *Privacy in context: Technology, policy, and the integrity of social life*. Stanford Law Books.

[34] Patrick Olivier and Peter Wright. 2015. Digital civics: taking a local turn. *Interactions* 22, 4 (2015), 61–63.

[35] Chanda Phelan, Cliff Lampe, and Paul Resnick. 2016. It's Creepy, But It Doesn'T Bother Me. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (CHI '16), ACM, New York, NY, USA, 5240–5251. DOI:https://doi.org/10.1145/2858036.2858381

[36] James Pierce. 2012. Undesigning Technology: Considering the Negation of Design by Design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '12), ACM, New York, NY, USA, 957–966. DOI:https://doi.org/10.1145/2207676.2208540

[37] Phillip Rogaway. 2015. The Moral Character of Cryptographic Work. *IACR Cryptol. EPrint Arch.* 2015, (2015), 1162.

[38] Saqib Saeed, Markus Rohde, and Volker Wulf. 2011. Analyzing Political Activists' Organization Practices: Findings from a Long Term Case Study of the European Social Forum. *Comput. Support. Coop. Work CSCW* 20, 4–5 (October 2011), 265–304. DOI:https://doi.org/10.1007/s10606-011-9144-0

[39] Pedro Sanches and Barry Brown. 2018. Data Bites Man: The Production of Malaria by Technology. In *Proceedings of the 19th ACM Conference on Computer Supported Cooperative Work and Social Computing*, ACM, New York, New York, USA.

[40] Pedro Sanches, Eric-Oluf Svee, Markus Bylund, Benjamin Hirsch, and Magnus Boman. 2013. Knowing Your Population: Privacy-Sensitive Mining of Massive Data. *Netw. Commun. Technol.* 2, 1 (April 2013). DOI:https://doi.org/10.5539/nct.v2n1p34

[41] Irina Shklovski and Nalini Kotamraju. 2011. Online contribution practices in countries that engage in internet blocking and censorship. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, ACM Press, New York, New York, USA, 1109. DOI:https://doi.org/10.1145/1978942.1979108

[42] Irina Shklovski and Nalini Kotamraju. 2011. Online contribution practices in countries that engage in internet blocking and censorship. In *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, ACM Press, New York, New York, USA, 1109. DOI:https://doi.org/10.1145/1978942.1979108

[43] Irina Shklovski, Janet Vertesi, Emily Troshynski, and Paul Dourish. 2009. The Commodification of Location: Dynamics of Power in Location-based Systems. In *Proceedings of the 11th International Conference on Ubiquitous Computing* (UbiComp '09), ACM, New York, NY, USA, 11–20. DOI:https://doi.org/10.1145/1620545.1620548

[44] Peter Ullrich and Philipp Knopp. 2018. Protesters' reactions to video surveillance of demonstrations: Counter-moves, security cultures, and the spiral of surveillance and counter-surveillance. *Surveill. Soc.* 16, 2 (2018), 183–202.

[45] Alexander Wilson, Mark Tewdwr-Jones, and Rob Comber. 2019. Urban planning, public participation and digital technology: App development as a method of generating citizen involvement in local planning processes. *Environ. Plan. B Urban Anal. City Sci.* 46, 2 (2019), 286–302.

[46] Volker Wulf, Konstantin Aal, Ibrahim Abu Ktesh, Meryem Atam, Kai Schubert, George P Yerousis, Dave Randall, and Markus Rohde. 2013. *Fighting against the Wall: Social Media use by Political Activists in a Palestinian Village*.

[47] Volker Wulf, Kaoru Misaki, Meryem Atam, David Randall, and Markus Rohde. 2013. "On the ground" in Sidi Bouzid. In *Proceedings of the 2013 conference on Computer supported cooperative work - CSCW '13*, ACM Press, New York, New York, USA, 1409. DOI:https://doi.org/10.1145/2441776.2441935

[48] Svetlana Yarosh and Svetlana. 2013. Shifting dynamics or breaking sacred traditions? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '13*, ACM Press, New York, New York, USA, 3413. DOI:https://doi.org/10.1145/2470654.2466468

[49] Zimmerman, Phil. 1991. Why I wrote PGP. *Why I Wrote PGP*. Retrieved September 18, 2019 from https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html

[50] Shoshana Zuboff. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *J. Inf. Technol.* 30, 1 (March 2015), 75–89. DOI:https://doi.org/10.1057/jit.2015.5

[51] 2019. What is Telegram and why was the app so popular during Hong Kong protests? *South China Morning Post*. Retrieved September 19, 2019 from https://www.scmp.com/tech/apps-social/article/3014382/what-telegram-and-why-did-messaging-app-prove-so-popular-during

[52] Irdeto Global Consumer Piracy Survey Report. Retrieved September 11, 2019 from https://resources.irdeto.com/piracy-cybercrime/irdeto-global-cusumer-piracy-survey-report

[53] Definition of SURVEILLANT. Retrieved September 18, 2019 from https://www.merriam-webster.com/dictionary/surveillant

[54] Google Researchers Found an Extremely Nasty iPhone Security Flaw. *Time*. Retrieved September 8, 2019 from https://time.com/5665298/iphone-security-apple-google/