LEUPHANA
UNIVERSITÄT LÜNEBURG

Resistance against cyber-surveillance within social movements and how surveillance adapts

Leistert, Oliver

Published in:
Surveillance and Society

DOI:
10.24908/ss.v9i4.4345

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

Link to publication

Citation for pulished version (APA):
Leistert, O. (2012). Resistance against cyber-surveillance within social movements and how surveillance adapts. *Surveillance and Society*, *9*(4), 441-456. https://doi.org/10.24908/ss.v9i4.4345

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 04. Dez.. 2025

Surveillance & Society

Article | Resistance against Cyber-Surveillance within Social Movements and how Surveillance Adapts

Oliver Leistert

Research Fellow, Center for Media and Communication Studies, Central European University Budapest. oleist@zeromail.org

Abstract

Activists around the world have developed practices and are taking distinct measures to resist cyber-surveillance. These range from using code words and taking out mobile phone batteries during meetings to the use of privacy enhancing technologies. This article discusses such measures by providing interviews with activists from a variety of countries, as well as by analyzing documents from German law enforcement agencies in a recent case against activists. These documents reveal that the meta-data produced via mobile telephony is at least as important for law enforcement as the content of the calls. Furthermore, if there is not enough meta-data, law enforcement will produce it to get to know the whereabouts of activists. This article thus argues that a mutual relationship between resistance and surveillance unfolds as one side reacts to the practices of the other: as soon as activists advance in the protection of their contents of telecommunication, the surveilling parties concentrate on meta-data to explore the whereabouts of their targets. To counter this threat only the discontinuation of mobile phone use has been articulated.

Introduction

> Actually, the problem here is mainly the killing of activists and journalists. The son of a press freedom icon, the leader of the alternative press during the Marcos years, his son was abducted two or three years ago and not yet released. It is suspected that he died (Eder / Manila).

Ederic Eder, founding member of Txt-Power, a civil society group set up after the Second People Power revolt in Manila in 2000 that is advocating free SMS in the Philippines, is pointing out the most drastic dangers of advocating press freedom. But even if it is not murder, from torture to soft repression to career endings, there are many risks involved when being an activist for a common cause. Perhaps all these risks can be limited if appropriate measures are taken with regard to how activists and advocates communicate. A fundamental issue for the needs and demands of activists remains the technology involved and its vulnerability to different kinds of breaches, which may stem from the lawful or unlawful interception of telecommunication. The outcome of such interceptions is generally used as a base for further profiling, and possibly leading to repression at some stage.

This article provides a detailed look at the practices on both sides: the surveilled and the surveilling parties. While my aim is not to generalize on the basis of what is presented here, the general outline argues in favor of the same problem globally: as activists develop mobile media practices that try to mitigate surveillance, such as by using code words or even encryption, the surveilling parties adapt as they have access to the telecommunication infrastructures used by activists and thus can access communication and the meta-data thereof in total secrecy. By showing this asymmetrical power relation in detail via

Leistert, Oliver. 2012. Resistance against Cyber-Surveillance within Social Movements and how Surveillance Adapts. *Surveillance & Society* 9(4): 441-456. http://www.surveillance-and-society.org | ISSN: 1477-7487
© The author(s), 2012 | Licensed to the Surveillance Studies Network under a Creative Commons Attribution Non-Commercial No Derivatives license.

interviews and a case study based on court documents, it becomes clear that as protest practice integrates mobile media into its domain of agency, the very same practice empowers the surveilling parties.

In the first part of this article, I recount a collection of statements given by activists that are engaged in fights and campaigns for social justice focusing on how activists protect themselves against digital surveillance or cyber-surveillance. The second part, by contrast, examines evidence provided to the courts in Germany in a recent §129a case, which since has been dropped. These documents provide valuable insight into the practices of state cyber-surveillance and as such give an indication of the successes and failures of the measures taken by activists for protection. What is more, it may be possible to draw out alternative measures based on this analysis.

The case study about the §129a case shows how much it is *meta-data* of telecommunication which compromises the telecommunications amongst activists. Of course, content is of interest for the surveilling parties, too. But as this case study shows, law enforcement agencies (LEAs) are even producing meta-data on their own to obtain a more finely granulated perspective on the whereabouts of those surveilled by sending silent SMS.

Therefore, whatever defensive practices the activists are developing with their mobile phones, whether it is using code words or using the phone only very rarely, the simple fact of having it switched on is enough to be followed. But while switching off the phone is the only way to remain under the radar, this practice then, as the case study shows, triggers much more suspicion leading to longer periods under surveillance.

By counterposing interview statements of activists in Part I with the documented practice of German LEAs, in Part II, I want to show that the technical infrastructure neatly serves as a surveillance infrastructure and that activists have no direct means to protect themselves from this threat but to switch off their devices. Thus, it would be appropriate to speak of mobile telephones as a hybrid, quasi dual-use technology that empowers and represses possibly at the same time. The relation of Parts I and II is mutually inclusive: As activists choose specific means to counter the surveillance scenario posed by mobile media while still maintaining the empowering aspects of it, LEAs also develop specific practices to make mobile media use in activism productive for them.

This is a dynamic within specific power relations and power struggles. Activists interviewed in Part 1 responded to surveillance by masking the *content* of their communication. But as Part II demonstrates, surveillance has iterated since and responds in a new way by targeting *meta-data* or data about the communication. This can be understood as a dialectical relation or a power dynamic as Fernandez and Huey (2009) suggest. They recommend that we "examine instances of resistance first, since they are likely going to be not only a response to surveillances practices but also present the new starting ground for the next set of surveillance mechanisms" (200). This article takes up just that challenge, and in some detail.

Also, it must be said that the question of the trustworthiness of telecommunication in general is nothing new and the history of efforts to secure communication is enormous and versatile (Kahn 1997). Writing when email, web and mobile telephony were still in a nascent state, two well-known scholars of cryptography, Landau and Diffie (1998), identified the potential impact on privacy as "profound."

> Telecommunications are intrinsically interceptable, and this interceptability has by and large been enhanced by digital technology. Communications designed to be sorted and switched by digital computers can be sorted and recorded by digital computers. Common-channel signaling, broadcast networks, and communication satellites facilitate interception on a grand scale previously unknown. Laws will not change these facts (226).

Today, this early warning sounds rather soft. The means and tools of cyber-surveillance have developed tremendously since the late 1990s. In a dramatic interplay between technological development, mass scale dissemination of digital devices, a rigorous shift in policy after 9/11 on a global scale, and the ongoing pressure for survival caused by a deregulated global economy, the issues stated by Landau and Diffie affect contemporary users of digital communication. Still, as I show, the "dual use" aspect of mobile telecommunication needs to be taken into much more serious consideration in future debates about the surveillance of mobile phones.

Activism and Digital Communication

> At any given moment we can be the subjects of surveillance. Police have the interest and the resources to practice surveillance. And there has recently been the creation of the cybernetic police on the federal level. There is also a similar entity in Mexico City. It is also well known that there are private technical teams, hired as mercenaries, to do these jobs. (Enrique / Mexico City)

For my current research I interviewed 50 activists from very different regions of the world about how they use mobile media[1] and about their thoughts on surveillance. Although from geographically and culturally distinct regions, all of them share the opinion that capitalism is systematically unjust and destructive and thus they all engage in efforts to overcome capitalism and build a more just society based on solidarity, and less mediated by financial means. Their activities span from human rights support to free public transportation actions; from providing non-commercial communication services for activists to running autonomous, non-state funded social centers; from providing free meals through *Food Not Bombs* to documenting police brutality; from solidarity work for prisoners to supporting small self-organized local unions of fishermen. They all share a critique of the concept of the vanguard and reject vertical and hierarchical organizations.

The exception are the interviewees from Pakistan, as these activists have all been engaged in what became known as the "Lawyers Movement" (Ahmed 2010, Malik 2008) or "Anti-Emergency Movement" (Bolognani 2010) and fought for an independent judiciary and the rule of law in Pakistan. Politically, this movement has been very heterogeneous and includes participants from different backgrounds.

In my interviews I was specifically interested in the general use of simpler mobile technologies, such as SMS, than in more advanced technologies like smart phones and the extended capabilities they provide. This has allowed me to turn my attention to a variety of places, including São Paulo, Mexico City, Oaxaca, Tokyo, Manila and Bangalore. Although methodological problems occur and need to be reflected when one wants to compare the use of mobile media by activists and social movements in these places, the benefit is a patchwork of reported experiences that in general show the same difficulties and unsolved issues for the safety of activists in all areas. Of course, political regimes, jurisdiction, and law enforcement agencies differ widely. Nonetheless, the technologies involved are essentially the same all around the globe. Additionally, the massive roll out of mobile phones in the Global South has changed and increased the activists' agency via mobile media as well. But still, I agree in many ways with what Christian Kreutz, a consultant for Information and Communication Technologies for Development, emphasizes:

> If one takes a look at the examples and different approaches of mobile activism, many potential developments can be identified. All these trends will rely not so much on technology, but much more on the activist's ideas for how to use mobile phones as a means of activism and on a critical mass of people participating (Kreutz 2010: 18).

[1] Mobile media is an umbrella term that includes devices from mobile phones to laptops and the way they are used, although most of the time mobile phones are the devices used as mobile media. Radio is not part of this research.

This article does not focus on the actual impact mobile media has on activists, which are manifold both in terms of changes in agency and in the transformation of patterns of exclusion and decision-making. However, it is possible to neglect the specificities of locations to some extent. I share the assumption that when a pattern of conduct (for example, the substantial enhancement of individual and collective autonomy by wireless communication capability) repeats itself in several studies in several contexts, we consider it plausible that the observation properly reflects the new realm of social practice (Castells *et al*. 2007: 3).

As SMS and basic mobile telephony are of special interest here, and on the other hand the infrastructure for mobile communications in all the regions I visited (except Japan) is compatible with or genuinely built on the Global System for Mobile Communications (GSM) standard, my findings can to some degree be generalized.

Taking Care about Content: Code Words and Written Words

Nearly all interviewees expressed strong concerns about the cyber-surveillance of their mobile and online communications. While very few stated because their activities were legal they do not have to fear cyber-surveillance, all of them still understood cyber-surveillance as a means to silence, censor and repress. It is noteworthy that regardless of the political regime under which they were active or human rights situation they were in, all activists decided to adopt specific measures to protect their activities and to safeguard the well-being of themselves and their colleagues. “We adjust. We change phones, although it is very expensive. For example, when there is a rally tomorrow, we say there is a festival tomorrow” (Mina, Minerva, Joan, Julie / Manila).

The use of code words can be seen as a ubiquitous practice in activists' mobile communications. This is not very surprising, as this cultural technique is as old as the struggles themselves. Still, it expresses a deep concern about being monitored and eavesdropped on regularly. As such, it signifies a mistrust that strongly contradicts legislation, which in general provides at least some privacy in telecommunications. Mistrust towards the effectiveness of legislation thus expresses an even deeper concern as it understands “the state” as a non-trustworthy entity, independent from what policy and laws proscribe. “Things that are very secret we don't talk about on the list. We then use some codes, like a call to a party, a lunch” (Legume / São Paulo). The list referred to is a simple mailing list, although run by an activist tech collective. Many activists I interviewed differentiate between spoken and written communications, well knowing that the latter are more easily intercepted and less costly, as digital content can be processed easily by computing, i.e. by searching for key words. “To protect the secrecy, people are encouraged to use the telephone. The email is written down, so it is very easy to be surveilled, but voice phone is only caught by wiretapping, which is rare” (Yasuda / Tokyo). No differentiation is made between online and mobile media. “We don't write anything about politics in SMS” (Non Collective / Manila).

But precautions taken can be much more substantial, leading to deliberate offline situations:

> Regarding mobile phone, if we have an action plan, and if we know the issue is sensitive or the movement is in a sensitive moment, we would not explicitly speak about it, and at the meeting, we take out all the batteries of the mobile phones until the meeting is over (Freddie / Hong Kong).

Mistrusting the devices one carries around all the time is clearly demonstrated by the fact that a good half of those interviewed, regardless of their region of activities, do not just turn off their device, but remove the battery. This is certainly a reasonable thing to do, although it is unclear whether mobile phones that are not specifically prepared can be activated and used as microphones remotely. Nonetheless, the safety gained is twofold: first, one goal of cyber-surveillance is to produce fear and suppress freedom of speech.

Therefore, any measure taken to feel safer is of high significance for political agency. Second, while one's own phone might not be the actual problem, those of others might be.[2]

These drastic measures resonate with Braman's (2006) observation that in general the expectation of privacy has decreased, which she understands as an increasing asymmetry of human beings and their agency to cope with advanced surveillance technologies:

> This loss of an actual expectation of privacy affects identity like other invasions of privacy do, but also provides a species-level challenge. As biological organisms, we still feel that if we pull the blinds and whisper, we will be private, though these actions are now irrelevant to the actuality; our senses and what we need to sense no longer operate at the same scale or level of granularity. Concerns about the impact of this trend include the likelihood of "anticipatory conformity" and decreased loyalty to a surveillance-driven government, as well as a chilling of association and free speech (Braman 2006: 130).

Although such technology can easily be rendered harmless by way of complete disconnection, the danger of offline surveillance remains. This is something an activist from Mexico, who prefers to remain anonymous,[3] unambiguously states:

> There was a time, when at a social center they had a sign on the wall and that said "turn off your phone and take the battery out." They established this rule that everyone that would go to a meeting had to turn off the phone and take the battery out. The reason being that if you turned off the phone and leave the battery in it, it could be used [so] that people would be able to listen to your conversation through your telephone. It was one of those things that I saw, where I thought: you should be more concerned what you talk in a local bar than taking the battery out of your cellphone (Anonymous / Mexico City).

As a general practice taking out batteries seems to be a very strong indicator of how ambivalent activists see mobile phones.

A critical use of mobiles and the knowledge when not to use them is instrumental for professional organizers, such as Saldanha from Bangalore, who is very active in rural areas in India:

> I try not to use my mobile for critical contents; I tend to use for that a landline. I prefer to meet people. Once we organized 5000 people: we got a call from the communities saying there is a public hearing and we need your help to mobilize and they gave us two days time. We arrived one day before the public hearing and we met with the key leaders. So we thought that is simple we just phone them but they said: no, don't do that, turn off your phone, I want you to go house to house, mobilize them. It worked, next day there were 5000 people. If we had done it through SMS, there would have been counter-mobilization. So tactically, it was useful not to use it. It is so much easier for the police to tap you than to go and stand and watch you (Saldanha / Bangalore).

Thus, undeniably a strategic use of mobile phones is key for political agency, which does not only choose amongst means of organizing, but may abandon mobile media altogether. In Oaxaca, Mexico, during the uprising of the teacher's union (APPO), which faced severe and deadly repression by federal police, the sheer availability of mobile telecommunications is already perceived dubiously:

---

2 It is worth mentioning that the iPhone's warranty is voided when users do this.

3 A lot of the interviewees either use pseudonyms or wanted to remain totally anonymous for the sake of their personal security—a demand that I fully comply with due to my research ethics.

> The mobile phone network was absolutely working during the 2006/2007 protests. Without interruptions. That is really strange, because Oaxaca was a strategic point of counterinsurgency and all this shit since 2006. In one minute they can shut down all the mobile phones, but they didn't. I don't know why. Maybe capitalism is bigger than we think. Here in Mexico, the boss of the cell phone networks is one of the richest in Mexico. Maybe in situations like this, surveillance and network are the same. This all is part of the contradiction (Blax / Oaxaca, Mx).

The asymmetric nature of surveillance also gives rise to interpretations of uncommon sounds and bursts as symptoms of surveillance. Unfamiliar noises and cracks during calls, for no apparent reason, are thus becoming a signifier of cyber-surveillance, although there is no hard proof of it.

> I am certain many of our phones are wiretapped, because weird things happen with the phone. Mainly because of things that have leaked and that could not have leaked otherwise. So, I am sure some phones are wiretapped. I am not sure what kind it is. During phone calls there are weird noises. Also when calling older activists (M / São Paulo).

The reality of eavesdropping on activists' communication lines is highlighted when, without public notice of a meeting, authorities are present at meeting points or activists are visited at home after some crucial phone calls they made. The connection of cracks during calls with subsequent real occurrences can still be wrong though as contemporary digital signals can be copied without any loss of quality—a different situation to analog telephony.

Beyond a strong embodied practice of what one should or should not say on the phone or write down in digital communications, and the distrust in general towards these digital devices, there are also more firm measures taken to safeguard communication amongst some activists, such as privacy enhancing technologies.

Privacy Enhancing Means

Securing telecommunications is a hard task. Although the application of common tools like PGP and GnuPG[4] is becoming more frequent amongst activists, very important issues remain unsolved. "We use GnuPG for email. We use TLS for the website" (Yasuda / Tokyo). An even more tech savvy activist states: "Encryption, in email TLS/SSL, in Jabber OTR and SSL, and VPN to access data. But I do not encrypt my emails by default, because 90 percent don't use email encryption" (Iokese / Madrid).

As large parts of the Global South lack access to the Internet for the average user and only few people have the financial means to use 3G phones, SMS remains the default solution for common telecommunications. In countries like India or the Philippines, SMS is reasonably cheap and affordable for large segments of the populations. But enhancing privacy of SMS remains largely unsolved. "If we can encrypt the messages we are sending, this would be very useful" (Mina, Minerva, Joan, Julie / Manila). Thus the mobile phone's use arguably remains limited for activists. "The mobile phone is used only regarding communication about having arrived somewhere—nothing else. In terms of Internet, we use PGP and for voice over IP we use Skype" (Francisco / Mexico City).

---

4 GnuPG, an open source software that allows users to encrypt and sign their data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. PGP is its non-open source version, from where email encryption for the masses started in the 1990s.

While activists are taking a variety of heterogeneous measures to make their telecommunication safer, the actual interest of the surveilling parties has shifted from the content of telecommunications to data that reveals over a longer period of time something different to the interceptors: meta-data. Recent initiatives by the European Union, for example, to retain meta-data of all telecommunications within the European Union for at least six months demonstrate the significance of such data to LEAs.[5] There is no satisfying way—at least technologically—to protect one from such surveillance schemes, mainly because this data is a necessary condition for most of the communication technologies involved to function. Thus Landau (2010) comments:

> It does not help to tell people to be secure. In order for their communications to be secure, security must be built into their communications systems. It must be ubiquitous, from the phone to the central office and from the transmission of a cell phone to its base station to the communications infrastructure itself (99).

All that is needed to identify patterns of communications, reconstruct social relations, places and times, frequent whereabouts, and much more, is computational powers and databases; very limited personnel is needed to collect and process meta-data. Not only does this meta-data facilitate analysis of the past but enables predictions about future whereabouts of activists. Only a few activists expressed any concerns about meta-data surveillance at all; they were largely unaware or had at best an imprecise idea about its implications. The powers of collected meta-data is nothing one can see at work easily. It is done elsewhere and symptoms of surveillance, be they imagined or not, like phones not working properly, do not occur from such measures. It is the infrastructure of telecommunications itself, which delivers such data, and the telecommunications providers are the voluntary or involuntary helping hands. The collection and analysis of a specific group's communication meta-data is done unobtrusively. Often it is collected without specific reason and never gets used for further investigations. The following example from Germany demonstrates that LEAs even produce such meta-data themselves to track down suspects' locations and movement.

Section 129a and the Case of "MG" in Germany: It's the Infrastructure, Stupid!

> So, the thing…around mobile phones that most shocked me was when it was revealed that the US carriers where surveilling citizens without warrants, AT&T and these things. That was a big knock. Not that I was that surprised, but that it was just so common. That really led me to thinking that surveillance is more of a day-to-day problem (Freitas / NYC).

To illustrate the contemporary possibilities for authorities to investigate and surveil with the help of telecommunication providers, the case of the German *MG* (*Militante Gruppe:* militant group) is insightful. The material shown here had been delivered to the courts for preliminary proceedings by the investigating authorities themselves. This makes them highly valuable in a specific sense: usually it is only possible to interpret symptoms of surveillance or be faced with its consequences, whereas here a documented account of such measures is available.[6] What conclusions the authorities made from this material is not of primary interest. Of much greater interest is what kind of surveillance had been used, how data had been received, what data was specifically produced to monitor and so forth. For the subject of cyber-surveillance only technical surveillance aiming at the telecommunication of the accused is represented here. Left aside are all other kinds of surveillance, like personal surveillance or video camera surveillance, which was conducted throughout all these years as well. What is more, details of the eavesdropping operations of phone calls are left out. It suffices to say that all calls to and from the accused's mobile and fixed-line

[5] See my discussion of this EU directive in Leistert 2008. A recent study by Frauenhofer Institute came to the conclusion that data retention does not significantly help law enforcement. See http://vds.brauchts.net/MPI_VDS_Studie.pdf.

[6] The material documented here is provided by sources that prefer to remain anonymous. These are parts of scanned paper pages produced by LEA's. The court reference numbers are GBA 2 BJs 58/06-2 and ST 45 / ST 14 – 140011/06.

phones had been intercepted, as well as those of relatives and friends. The number of people affected by surveillance operations adds up to more than 200, even though there were only three suspects.

The primary purpose of presenting this material is to demonstrate the weakness of telecommunication infrastructure with regards to privacy. This example is illustrative as no legal obstacles prevented the surveilling parties from their work in any way, due to the application of the anti-terror law §129a. These surveillance operations are presented here on a level of documented evidence and demonstrate, in a nutshell, the technical possibilities of the telecommunication surveillance unleashed.

Section 129 of the German Criminal Code

Some context is needed beforehand: in Germany, law enforcement's legal means for infiltrating, surveying and detaining political opponents after World War II have been steadily extended since the 1970s. The most prominent is §129a of the criminal code, dealing with terrorist organizations. Its older variant §129 deals with criminal organizations and actually predates the Federal Republic of Germany. It was extensively abused during the Nazi era for the persecution of imagined or real opponents. Only a few years later in the 1950s, hundreds of investigations against alleged communists and activists opposing the rearmament of West Germany were performed applying this controversial paragraph. Subsequently §129a was introduced, covering terrorist organizations in the 1970s, and after 9/11 §129b was introduced, dealing with foreign terrorist organizations.[7] These laws basically strip suspects of every last bit of their (privacy) rights and have been used effectively by LEAs most frequently to update their knowledge on leftist activists. Hardly any of the numerous §129a investigations made it to court. More than 95% are silently shut down, often after years of very intense surveillance.[8]

The introduction of this paragraph in the 1970s was amongst other means meant to deal with the Red Army Fraction (RAF) and the Revolutionary Cells (RZ).[9] Although these actors now belong to the past, the paragraph has continued to see numerous applications to investigate leftist or social justice groups.[10] The application of §129(a,b) allows far-reaching surveillance not only of those under suspicion, but also of those who have been in contact with those under suspicion—even if only once. As the suspects are commonly engaged in a diversity of political fields, the application of such an investigation produces a complex reproduction of the social net of many politically active people, regardless if they are themselves suspects defined under the investigation or not. Sharing a flat, belonging to the family or working at the same company is enough to become a target of extensive surveillance once §129(a,b) is at work.

The MG Investigations

The MG investigations, into the alleged terrorist group known by these initials, started in 2001 (with some pre-proceedings by the German secret service since 1998). Amongst the many different allegations were

---

7 An official English translation of the German criminal code incl. §129 can be found at http://www.gesetze-im-Internet.de/englisch_stgb/englisch_stgb.html. But the surveillance means allowed to deploy are defined in the code of criminal procedure (Strafprozessordnung, StPO). Especially StPO §110a (surveillance of telephone and post), §100c and §163 (long-ongoing observations), §110a, §110c (systematic deploying of undercover agents and spies), and again §100c (surveillance of acoustics and images inside private homes) give almost unrestricted powers to LEAs. An English translation of the StPO can be found at http://www.gesetze-im-Internet.de/englisch_stpo/index.html.

8 The surveillance conducted under these paragraphs does not always seek to remain unnoticed. The suspects thus react to the investigations and provide the LEAs further insights into their social net. Additionally, suspects reportedly have lost jobs and suffered as well psychologically from investigations. As such this is highly problematic as this all happens even before pre-trial confinement.

9 Both were using force to achieve political goals, the big difference is that the RAF, whose founding generation is known as Baader-Meinhof-Group, went underground whereas the RZ personnel had their normal day job while pursuing RZ activities at night. Their genealogy can be traced back to the events of 1968, in part even until the protest against the rearmament of West-Germany in 1955, which was a big debate at the time.

10 Right-wing groups are very rarely targets of §129(a,b) although violence originating from right wing groups in Germany, especially against humans, including murder, continues since Germany's reunification.

attacks on German military equipment. The material shown here is from the so-called "MG 1" investigation, which started in 2001 and ended in 2008. Others are still pending, as there have been numerous different investigations.[11] The surveilled had been accused of forming a terrorist group. None of the accused in this case have been sentenced and the case never become a regular court case.[12] Additionally, on March 11 2010, the Federal Supreme Court (BGH) ruled that the entire set of procedures used by the LEAs in this case (MG1), had been unlawful and that the surveillance conducted was not appropriate as there never was a reasonable enough suspicion.[13] The data collected nonetheless remains in the police archives and has recently been transferred to the Berlin criminal state police.

In the following passages, some details about the surveillance operations are explained. Translations are by the author.

Retained Meta-Data of (Mobile-)Telephony

Figure 1 shows a typical *Auskunftsersuchen* (request for information), which reports call data from 1.10.2006 to 31.3.2007 (only 3.10. to 19.10.2010 is shown here, but the astonishingly long duration of five months is mentioned in the upper left area) from one MSISDN.[14] Besides the number dialed, other information is printed: MCC[15] 266 refers to Germany, MNC[16] 01 refers to T-Mobile, the MSC-ID[17] is responsible for the end-to-end connection, e.g. allowing hand-over requirements during the call. The Cell-ID references the actual cell which the phone was logged in, and on the far right, geographical positions of this cell-ID are printed. Generally all telephone communication meta-data to and from the mobile phones of the suspects had been retained and provided to the authorities. These meta-data include, amongst other rather pure technical parameters, the phone numbers, the IMSI[18] (if applicable), duration of call, type of call (it differentiates between service call types), and the geo-coordinates of the cell where the client was connected. This means that during any communication over the phone, its geo-coordinates reveal the location of the person that used it. From a technical perspective the same meta-data is produced by both successful and failed connections. Thus, unsuccessful communication also provides value for the surveillance operations.

---

11 Details about the cases, their timelines and each investigation are published at https://einstellung.so36.net.

12 Anne Roth, partner and mother of the children of one suspect in these investigations, Andrej Holm, has been blogging extensively about her life under total surveillance. Here, stunning details are published, partly in English http://annalist.noblogs.org.

13 The rule is online (German only): http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.pyGericht=bgh&Art=en&sid=52c1c2b856536c08dab95908724bccfd&nr=52160&pos=0&anz=1

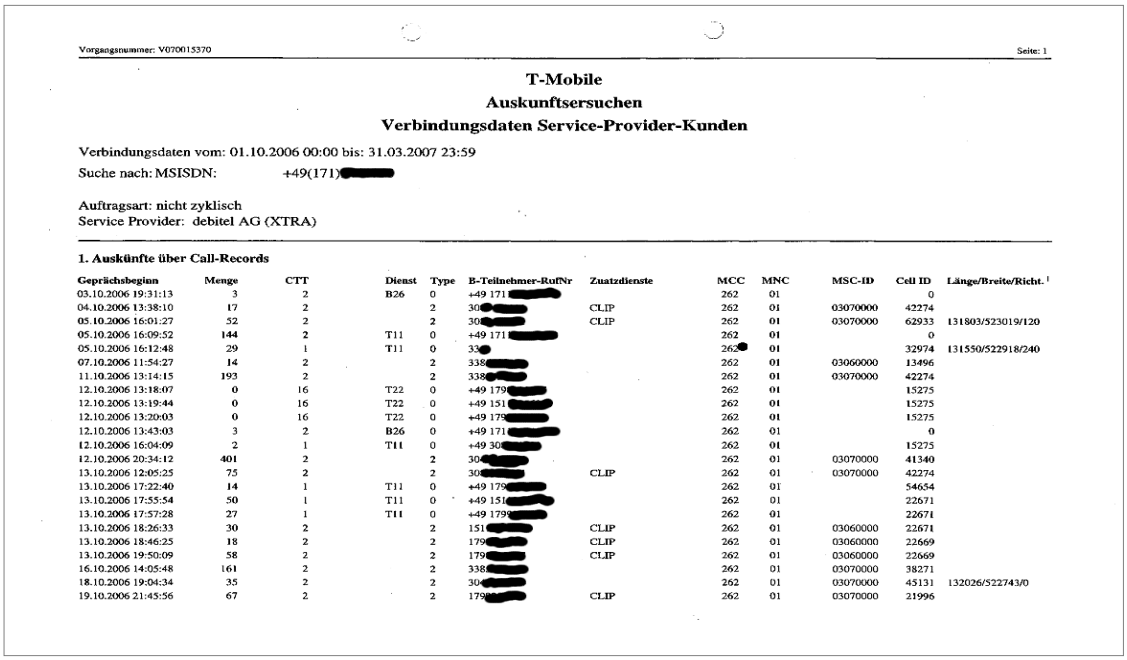
14 The MSISDN is a worldwide unique number for calling and use of a mobile phone.

15 A code defined by the ITU to identify countries of mobile phones. It is a part of the IMSI.

16 A code to uniquely identify a mobile phone operator/carrier using one of the common mobile communications standards such as GSM.

17 The MSC is the primary service delivery node for GSM/CDMA, responsible for routing voice calls and SMS as well as other services. The MSC sets up and releases the end-to-end connection, handles mobility and hand-over requirements during the call and takes care of charging and real time prepaid account monitoring

18 IMSI is the International Mobile Subscriber Identity, a unique number which identifies a SIM card. SIM cards often link to the user's name.



Vorgangsnummer: V070015370 Seite: 1

T-Mobile
Auskunftsersuchen
Verbindungsdaten Service-Provider-Kunden

Verbindungsdaten vom: 01.10.2006 00:00 bis: 31.03.2007 23:59
Suche nach: MSISDN: +49(171)[redacted]

Auftragsart: nicht zyklisch
Service Provider: debitel AG (XTRA)

1. Auskünfte über Call-Records

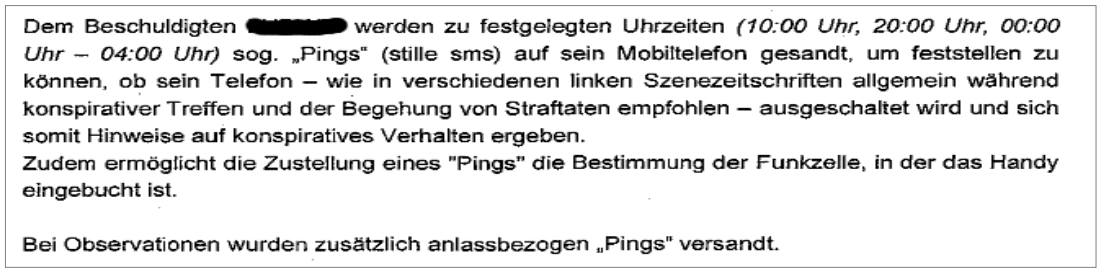
Gesprächsbeginn	Menge	CTT	Dienst	Type	B-Teilnehmer-RufNr	Zusatzdienste	MCC	MNC	MSC-ID	Cell ID	Länge/Breite/Richt.
03.10.2006 19:31:13	3	2	B26	0	+49 171[redacted]		262	01		0	
04.10.2006 13:38:10	17	2		2	30[redacted]	CLIP	262	01	03070000	42274	
05.10.2006 16:01:27	52	2		2	30[redacted]	CLIP	262	01	03070000	62933	131803/523019/120
05.10.2006 16:09:52	144	2	T11	0	+49 171[redacted]		262	01		0	
05.10.2006 16:12:48	29	1	T11	0	33[redacted]		262	01		32974	131550/522918/240
07.10.2006 11:54:27	14	2		2	338[redacted]		262	01	03060000	13496	
11.10.2006 13:14:15	193	2		2	338[redacted]		262	01	03070000	42274	
12.10.2006 13:18:07	0	16	T22	0	+49 179[redacted]		262	01		15275	
12.10.2006 13:19:44	0	16	T22	0	+49 151[redacted]		262	01		15275	
12.10.2006 13:20:03	0	16	T22	0	+49 179[redacted]		262	01		15275	
12.10.2006 13:43:03	3	2	B26	0	+49 171[redacted]		262	01		0	
12.10.2006 16:04:09	2	1	T11	0	+49 30[redacted]		262	01		15275	
12.10.2006 20:34:12	401	2		2	30[redacted]		262	01	03070000	41340	
13.10.2006 12:05:25	75	2		2	30[redacted]	CLIP	262	01	03070000	42274	
13.10.2006 17:22:40	14	1	T11	0	+49 179[redacted]		262	01		54654	
13.10.2006 17:55:54	50	1	T11	0	+49 151[redacted]		262	01		22671	
13.10.2006 17:57:28	27	1	T11	0	+49 179[redacted]		262	01		22671	
13.10.2006 18:26:33	30	2		2	151[redacted]	CLIP	262	01	03060000	22671	
13.10.2006 18:46:25	18	2		2	179[redacted]	CLIP	262	01	03060000	22669	
13.10.2006 19:50:09	58	2		2	179[redacted]	CLIP	262	01	03060000	22669	
16.10.2006 14:05:48	161	2		2	338[redacted]		262	01	03070000	38271	
18.10.2006 19:04:34	35	2		2	30[redacted]		262	01	03070000	45131	132026/522743/0
19.10.2006 21:45:56	67	2		2	179[redacted]	CLIP	262	01	03070000	21996	

Figure 1

Locational Surveillance via Silent SMS

A surveillance tool used very intensely in these investigations by German LEAs is silent SMS (also referred to as "ping"). Besides eavesdropping on telephony, silent SMS was used extensively to identify the person's location and whether the mobile phone is switched on or off.[19] What is a silent SMS? A silent SMS is sent to a mobile phone to obtain location data, the approximate whereabouts of the device. A silent SMS does not notify the receiver of its emergence and contains no content data—it is not perceivable to the user. But as it is an SMS in the technical sense: it generates meta-data, which then provides insights about the whereabouts of the phone. Figure 2 explains one schedule of sending silent SMS and the LEAs' reasons for doing so. The number of silent SMS sent during the whole investigation is in the range of tens of thousands. They were all sent by the authorities themselves to generate connection data, which the LEAs then requested from the telecommunication providers. The delay between request and reception of connection data varied between one week and one month. Thus, silent SMS is a measure for long-term surveillance. Figure 3 is an evaluation of silent SMS's sent hourly to one mobile phone.

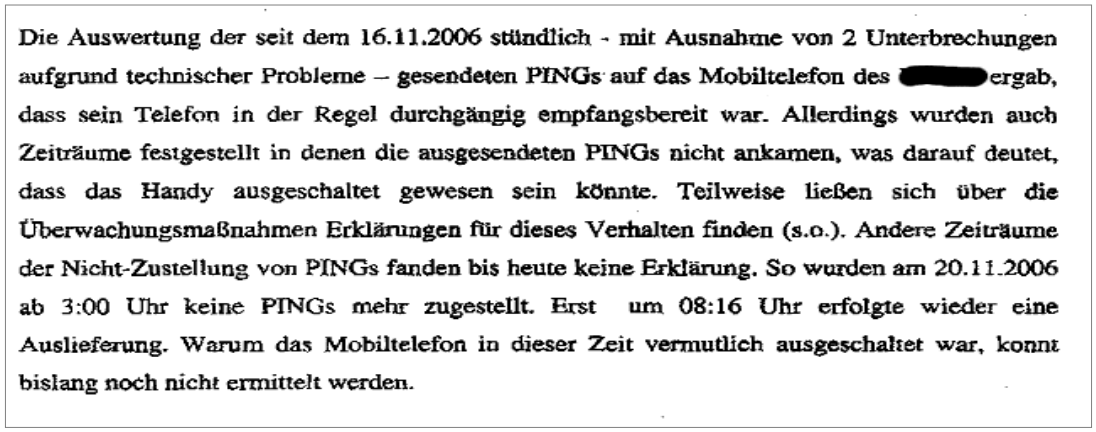
[19] The latter usually leads the authorities to the assumption that if the accused switched off her phone, she is suspicious of preparing or committing a crime.



Dem Beschuldigten [redacted] werden zu festgelegten Uhrzeiten *(10:00 Uhr, 20:00 Uhr, 00:00 Uhr – 04:00 Uhr)* sog. „Pings" (stille sms) auf sein Mobiltelefon gesandt, um feststellen zu können, ob sein Telefon – wie in verschiedenen linken Szenezeitschriften allgemein während konspirativer Treffen und der Begehung von Straftaten empfohlen – ausgeschaltet wird und sich somit Hinweise auf konspiratives Verhalten ergeben.
Zudem ermöglicht die Zustellung eines "Pings" die Bestimmung der Funkzelle, in der das Handy eingebucht ist.

Bei Observationen wurden zusätzlich anlassbezogen „Pings" versandt.

Figure 2
On predefined times (10:00h, 20:00h, 00:00h - 4:00h) so called "Pings" (silent SMS) are being sent to the accused mobile phone to evaluate if his phone—as recommended in various leftist scene publications generally during conspiratorial meetings and during committing a crime—is switched off and thus hints towards conspiratorial behavior. Additionally, the delivery of a "ping" allows for identification of the cell, which the phone is logged into.
During observations, additional event-related "pings" have been sent (Author trans).



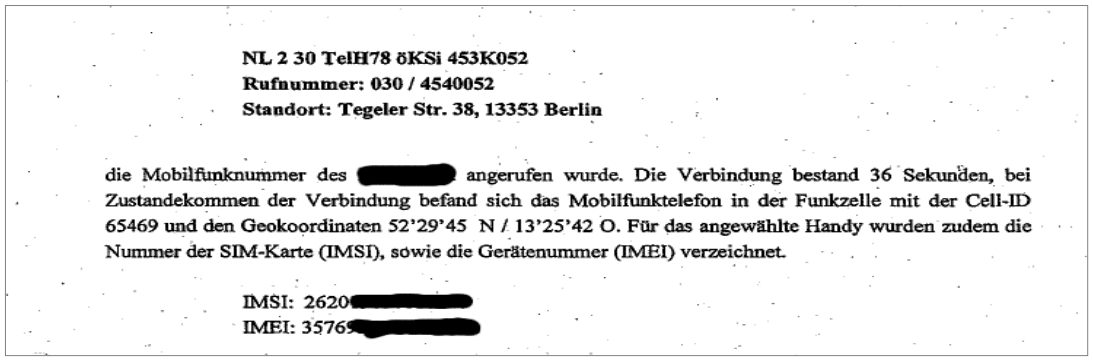
Die Auswertung der seit dem 16.11.2006 stündlich - mit Ausnahme von 2 Unterbrechungen aufgrund technischer Probleme – gesendeten PINGs auf das Mobiltelefon des [redacted] ergab, dass sein Telefon in der Regel durchgängig empfangsbereit war. Allerdings wurden auch Zeiträume festgestellt in denen die ausgesendeten PINGs nicht ankamen, was darauf deutet, dass das Handy ausgeschaltet gewesen sein könnte. Teilweise ließen sich über die Überwachungsmaßnahmen Erklärungen für dieses Verhalten finden (s.o.). Andere Zeiträume der Nicht-Zustellung von PINGs fanden bis heute keine Erklärung. So wurden am 20.11.2006 ab 3:00 Uhr keine PINGs mehr zugestellt. Erst um 08:16 Uhr erfolgte wieder eine Auslieferung. Warum das Mobiltelefon in dieser Zeit vermutlich ausgeschaltet war, konnt bislang noch nicht ermittelt werden.

Figure 3
The evaluation of the hourly sent (since 16.11.2006) PING's to the mobile phone of XX showed that his phone had been able to receive SMS generally. Nonetheless there have been time frames where the sent pings did not arrive, which might mean that the phone has been switched off. In part this can be explained by other surveillance measures taken. Other unsuccessful deliveries of pings can still not be explained as on the 20.11.2006 from 3:00AM onwards until 08:16AM no pings could be delivered. Until now it has not been clarified why the mobile phone has been switched off during this time (Author trans).

Evaluating Individual Calls

A common practice among activists is to change SIM Cards to obtain a new number and thus a new profile. Figure 4 and Figure 5 show that both the SIM card related IMSI and the device related IMEI[20] are transmitted in the network and thus used by authorities. In Figure 4, the LAC denotes the whereabouts of the phone in a numerical code. Figure 5 is a precise description about one single call (duration 36 seconds), referencing the address of the public phone booth that was used, the duration of call, cell ID the mobile was logged into, the geo-coordinates of this cell and the mobile phone's IMSI and IMEI.

[20] IMEI is the International Mobile Station Equipment Identity, a 15-digits long, unique serial number, which makes it possible to identify any GSM or UMTS client.

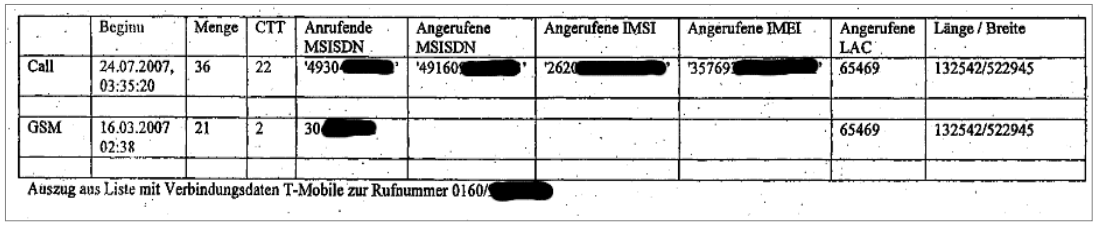


NL 2 30 TelH78 öKSi 453K052
Rufnummer: 030 / 4540052
Standort: Tegeler Str. 38, 13353 Berlin

die Mobilfunknummer des [redacted] angerufen wurde. Die Verbindung bestand 36 Sekunden, bei Zustandekommen der Verbindung befand sich das Mobilfunktelefon in der Funkzelle mit der Cell-ID 65469 und den Geokoordinaten 52'29'45 N / 13'25'42 O. Für das angewählte Handy wurden zudem die Nummer der SIM-Karte (IMSI), sowie die Gerätenummer (IMEI) verzeichnet.

IMSI: 2620[redacted]
IMEI: 35769[redacted]

Figure 4
[From this public phone] the mobile number of XX has been called. The call time was 36 seconds, when the connection started the mobile phone was logged into the cell with the Cell-ID 65469 at the geo-coordinates 52'29'45 N / 13'25'42 E. IMSI and IMEI from the called mobile phone were recorded(Author trans).

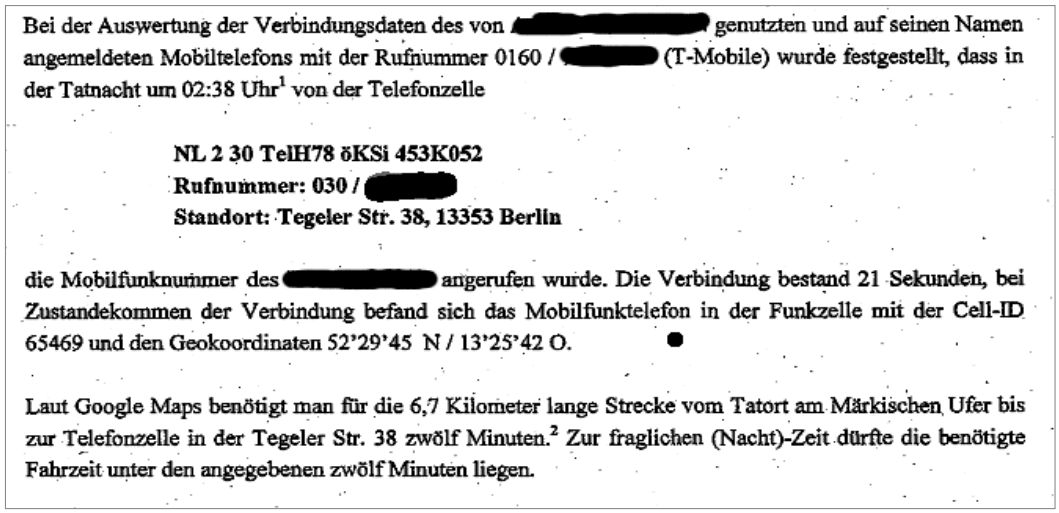


	Beginn	Menge	CTT	Anrufende MSISDN	Angerufene MSISDN	Angerufene IMSI	Angerufene IMEI	Angerufene LAC	Länge / Breite
Call	24.07.2007, 03:35:20	36	22	'4930[redacted]'	'49160[redacted]'	'2620[redacted]'	'35769[redacted]'	65469	132542/522945
GSM	16.03.2007 02:38	21	2	30[redacted]				65469	132542/522945

Auszug aus Liste mit Verbindungsdaten T-Mobile zur Rufnummer 0160/[redacted]

Figure 5

Figure 6 evaluates data from one specific call, generated on a special day, on which a militant action in Berlin took place. It is calculated (via Google Maps) that the average travel time from the crime site to the public phone booth from where the surveilled mobile phone was called, allows for the possibility that the person that used the public phone also committed the crime.



Bei der Auswertung der Verbindungsdaten des von [redacted] genutzten und auf seinen Namen angemeldeten Mobiltelefons mit der Rufnummer 0160 / [redacted] (T-Mobile) wurde festgestellt, dass in der Tatnacht um 02:38 Uhr[1] von der Telefonzelle

NL 2 30 TelH78 öKSi 453K052
Rufnummer: 030 / [redacted]
Standort: Tegeler Str. 38, 13353 Berlin

die Mobilfunknummer des [redacted] angerufen wurde. Die Verbindung bestand 21 Sekunden, bei Zustandekommen der Verbindung befand sich das Mobilfunktelefon in der Funkzelle mit der Cell-ID 65469 und den Geokoordinaten 52'29'45 N / 13'25'42 O.

Laut Google Maps benötigt man für die 6,7 Kilometer lange Strecke vom Tatort am Märkischen Ufer bis zur Telefonzelle in der Tegeler Str. 38 zwölf Minuten.[2] Zur fraglichen (Nacht)-Zeit dürfte die benötigte Fahrzeit unter den angegebenen zwölf Minuten liegen.

Figure 6

During the evaluation of connection data of the mobile phone used by XX and registered under his name with the call number 0160 / XXXXXX (T-Mobile) it was discovered that during the night of the crime at 02:38h [from this public phone] the mobile number of XX has been called. The call time was 21 seconds, when the connection started the mobile phone was logged into the cell with the Cell-ID 65469 at the geo-coordinates 52'29'45 N / 13'25'42 E.
According to Google Maps it takes twelve minutes to travel the 6.7 km distance from the crime scene at Märkisches Ufer to the public phone at Tegeler Strasse 38. At night time the travel time should be under the

Email Interception

As the accused subscribed to numerous email lists, hundreds to thousands of emails went straight to the authorities during 2001 and 2008. This is an easy task for LEAS, given the uncomplicated matter of getting access to email accounts of service providers such as GMX or Yahoo! Interestingly, as Figure 7 reveals, PGP encrypted emails could not be read. The email's subject of course is plain text, as well as its meta-data. It states: "Four more PGP-encrypted emails have been found, whose subjects refer to the event in Trier. Nothing can be said about the contents of these e-mails."

Es wurden vier weitere PGP-verschlüsselte E-Mails festgestellt, die sich vom Betreff her mit der Veranstaltung in Trier beschäftigen. Zum Inhalt dieser Mails kann keine Aussage getroffen werden.

Figure 7

Cross-Referencing of Eavesdropping and Cell Logs

Figure 8 shows how both the results of eavesdropping and data about a cell a mobile phone logged into are combined to evaluate one situation on one particular evening.

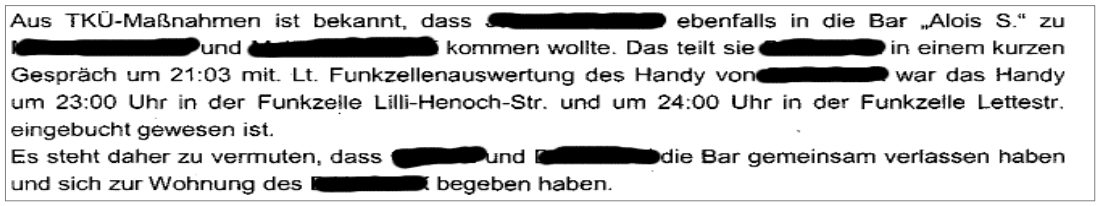

Aus TKÜ-Maßnahmen ist bekannt, dass [redacted] ebenfalls in die Bar „Alois S." zu [redacted] und [redacted] kommen wollte. Das teilt sie [redacted] in einem kurzen Gespräch um 21:03 mit. Lt. Funkzellenauswertung des Handy von [redacted] war das Handy um 23:00 Uhr in der Funkzelle Lilli-Henoch-Str. und um 24:00 Uhr in der Funkzelle Lettestr. eingebucht gewesen ist.
Es steht daher zu vermuten, dass [redacted] und [redacted] die Bar gemeinsam verlassen haben und sich zur Wohnung des [redacted] begeben haben.

Figure 8

From eavesdropping operations it is known that XX as well wanted to come to the pub "Alois S." to meet with XX and XX. This she told XX in a short phone call at 21:03h. According to the evaluation of cells the mobile phone of XX was logged in, it was logged into the cell Lillie-Henoch-Street at 23.00h and Lettestreet at 24:00h. Therefore it is reasonable that XX and XX left the bar together and went to the apartment of XX (Author trans).

Figure 9 states the wide knowledge the surveilling parties gathered about the suspects' social network, their activities and what the sister of one suspect said. Switching off one's mobile phone is interpreted as conspiratorial behavior. The document provided here is actually written to get permission for a prolongation of the surveillance operations. With only very few modifications it has been used over and over again to get these permissions from a judge. It references a combination of eavesdropping on telephone calls and cell log data (obtained through silent SMS most likely).

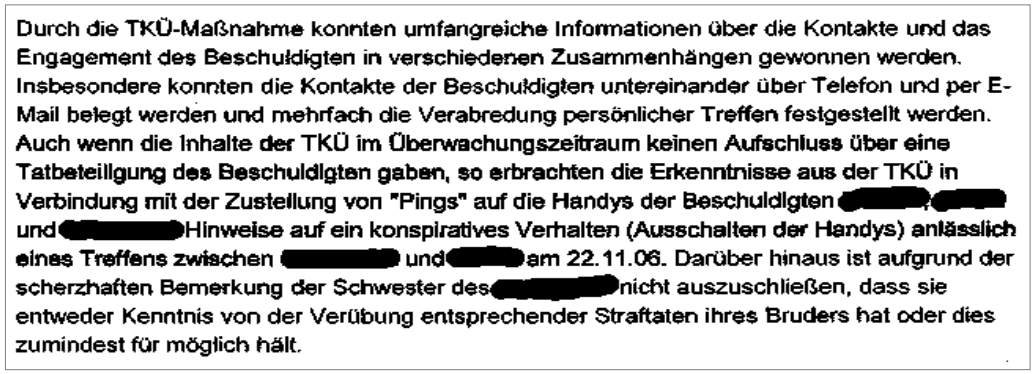

Durch die TKÜ-Maßnahme konnten umfangreiche Informationen über die Kontakte und das Engagement des Beschuldigten in verschiedenen Zusammenhängen gewonnen werden. Insbesondere konnten die Kontakte der Beschuldigten untereinander über Telefon und per E-Mail belegt werden und mehrfach die Verabredung persönlicher Treffen festgestellt werden. Auch wenn die Inhalte der TKÜ im Überwachungszeitraum keinen Aufschluss über eine Tatbeteiligung des Beschuldigten gaben, so erbrachten die Erkenntnisse aus der TKÜ in Verbindung mit der Zustellung von "Pings" auf die Handys der Beschuldigten [redacted] und [redacted] Hinweise auf ein konspiratives Verhalten (Ausschalten der Handys) anlässlich eines Treffens zwischen [redacted] und [redacted] am 22.11.06. Darüber hinaus ist aufgrund der scherzhaften Bemerkung der Schwester des [redacted] nicht auszuschließen, dass sie entweder Kenntnis von der Verübung entsprechender Straftaten ihres Bruders hat oder dies zumindest für möglich hält.

Figure 9

Extensive information could be gathered by eavesdropping of telephone about the contacts and the engagement of the accused in different interrelationships. Specifically the contacts of the accused amongst themselves via telephone and email could be proven and multiple personal meetings have been identified. Even if the contents of the eavesdropping during the time of surveillance did not provide details about participation of the accused in the crimes, still, the results from the eavesdropping operations in relation with the transmission of "Pings`` to the mobile phone of the accused XX and XX showed conspiratorial behavior (switching off the mobile phone) on the occasion of a meeting of XX and XX on the 22.11.06. Additionally, due to the joke of the sister of XX, it cannot be excluded that she either knows about her brother committing such crimes or at least thinks it is possible (Author trans.).

Conclusion

In essence, activists can and in part do secure their communication contents, but this still provides enough information about their social networks: who is communicating with whom, when and where. Even how long and by which media technology. It is the infrastructure that provides these insight, as it needs such

meta-data for its operation. All the examples given above regarding the surveillance operations on the suspects point to the infrastructure as the source of interception. The infrastructure offers a very good point of interception without much risk of detection. When communication was encrypted client to client, its contents were secured against this surveillance scheme, as Figure 7 showed. That location information was actively generated by sending a very high number of silent SMS over a long duration additionally points to the strategic importance of the cellular network for LEA's.

The location data on the whereabouts of the suspects provided by the suspect's mobile phone are sufficiently precise for the LEAs to capture on an hourly, weekly or monthly basis. In a city like Berlin, mobile phone cells are densely rolled out. Thus, the location data can be as exact as the functional radius of the cell.

The location data provided with silent SMS and cell log data generates a history of the suspect's travel route and whereabouts on an hourly frequency. Once the mobile phone had been switched off (or the battery was empty), this triggered an alert for the authorities and these time frames then were considered conspiratorial behavior. This is a common practice of activists to defend themselves against surveillance. As they are securing themselves by removing batteries, the LEAs in the documented case used this practice over and over again to infer conspiratorial behavior and thus to get prolongations for their surveillance operations from the courts.

Comparing security considerations of the activists interviewed and the practice of the German LEA in the MG investigation shows that no real measures, besides email encryption and switching off phones, are readily available to keep mobile communications an effective and secure tool without risking the inherent support of surveillance operations. The strong accounts provided by meta-data about the social networks of the suspects (who called whom and when and where) can hardly be countered.

The nature of the relationship between resistance to surveillance and the answers of surveillance practice to these kinds of resistance practices can be understood as dialectical. Activists use code words, limit mobile phone use and even use encryption. The surveillance practice thus turns to meta-data analysis and even produces them, as in the case of silent SMS. If resistance goes so far as to dismiss the use of mobile telephony altogether by switching the phones off, LEAs' surveillance practice answers by prolonging their surveillance activities with the argument that it is suspicious if activists switch off their phones even though there is no reliable evidence of criminal activity.

The relation of resistance and surveillance can be seen as circular or spiral: once one side re-empowers itself by technical measures, the other finds new ways to gather information or hide better their activities. There is a limit here, of course, which is the loss of agency: in a society that relies on telecommunications, activism cannot dismiss their use completely. Avoiding or minimizing the use of mobile phones can inhibit agency; similarly, too many security measures can hamper the effectiveness of activism.

It is the infrastructure of mobile telephony that can be subverted and turned against its users by sending hourly "pings" to the mobile phones of suspects. As the technical infrastructure is the core element of mobile telephony there are only limited ways to contain this scenario from an activist's perspective: changing phones and SIM cards regularly reduces the risk of identification. Another measure is to tactically engage in this containment. Switching off the phones randomly and not only strategically; mailing one's switched on phone to another place or other playful engagements re-empower the users of mobile phones. Once such a set of practices is established as a common activity, surveillance would need to catch up again.

As the critical point of surveillance is the infrastructure of telecommunications, alternatives to the rolled-out infrastructures, run by trustworthy partners, suggest a solution. If this infrastructure is run by such

trustworthy partners, maybe as well from the activist domain, and the activists encrypt the content client to client, the costs of surveillance rise and the personnel that has the expertise to surveil needs to be highly specialized.

Getting off the mobile phone's network can be achieved as well by strictly using the Internet via wireless LAN (and not through the data plan of the mobile provider). This is not secure per se but it bears characteristics that make it a promising candidate for trustworthiness. Strictly using the Internet via wireless LAN, either for messaging or voice call, multiplies the necessary points of interception as the Internet is much more decentralised than a mobile phone network. Additionally, its layers and stacks are accessible as it is a more open design than the mobile phone network. The consequences are a multitude of technological solutions for privacy enhanced communications in the open source realm. Thus, anonymity and encryption are useful tactics that can be incorporated into the communication practices of larger groups.

Acknowledgements

I thank two anonymous reviewers for important comments and the editors of this edition of *Surveillance & Society*: Kate Milberry, Andrew Clement, and Colin Bennett. Additionally for support I thank Lina Dencik and the Center for Media and Communication Studies at CEU, Budapest.

Interviews

Anonymous / Mexico City. 2009. Interview with the author, Mexico City, 28.8.2009. Unpublished transcript of audio recording.
Blax / Oaxaca (Mx). 2009. Interview with the author, Oaxaca, 2.9.2009. Unpublished transcript of audio recording.
Eder / Manila. 2009. Interview with the author, Manila, 3.10.2009. Unpublished transcript of audio recording.
Enrique / Mexico City. 2009. Interview with the author, Mexico City, 28.9.2009. Unpublished transcript of audio recording.
Francisco / Mexico City. 2009. Interview with the author, Mexico City, 4.9.2009. Unpublished transcript of audio recording.
Freddie / Hong Kong. 2009. Interview with the author, Tokyo, 25.9.2009. Unpublished transcript of audio recording.
Freitas / NYC. 2009. Interview with the author, New York City, 12.8.2009. Unpublished transcript of audio recording.
Iokese / Madrid. 2009. Interview with the author, Madrid, 4.12.2009. Unpublished transcript of audio recording.
Legume / São Paulo. 2009. Interview with the author, São Paulo, 29.7.2009. Unpublished transcript of audio recording.
M / São Paulo. 2009. Interview with the author, São Paulo, 29.7.2009. Unpublished transcript of audio recording.
Mina, Minerva, Joan, Julie / Manila. 2009. Interview with the author, Manila, 3.10.2009. Unpublished transcript of audio recording.
Non Collective / Manila. 2009. Interview with the author, Manila, 2.10.2009. Unpublished transcript of audio recording.
Saldanha / Bangalore. 2009. Interview with the author, Bangalore, 17.10.2009. Unpublished transcript of audio recording.
Yasuda / Tokyo. 2009. Interview with the author, Tokyo, 19.9.2009. Unpublished transcript of audio recording.
Zaman / Lahore. 2009. Interview with the author, Lahore, 27.10.2009. Unpublished transcript of audio recording.

References

Ahmed, Zahid Shaha. 2010. Fighting for the rule of law: civil resistance and the lawyers' movement in Pakistan. *Democratization* 17(3*):* 492-513.
Bolognani, Marta. 2010. Virtual protest with tangible effects? Some observations on the media strategies of the 2007 Pakistani anti-Emergency movement. *Contemporary South Asia* 18(4): 401-412
Braman, Sandra. 2006. *Change of State: Information, Policy, and Power*. Cambridge: MIT Press.
Castells, Manuel, Mireira Fernandex-Ardevol, Jack Linchuan Qui and Araba Sey. 2007. *Mobile Communication and Society: A Global Perspective*. Cambridge: MIT Press.
Fernandez, Luis A. and Laura Huey. Is Resistance Futile? Some Thoughts on Resisting Surveillance. *Surveillance & Society* 6(3): 198-202.
Kahn, David. 1996. *The Codebreakers: the story of secret writing*. New York: Scribner.
Kreutz, Christian. 2010. Mobile activism in Africa: Future Trends and Software Developments. In *SMS Uprising - Mobile Activism in Africa*, ed E. Ekine, 17 – 31. Cape Town, Nairobi: Pambazuka Press.
Landau, Susan. 2010. *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*. Cambridge: MIT Press.
Landau, Susan and Whitfield Diffie. 1998. *Privacy on the Line. The Politics of Wiretapping and Encryption*. Cambridge: MIT Press.
Leistert, Oliver. 2008. Data Retention in the European Union: When a Call Returns. *International Journal of Communications* 2, 925–35.
Malik, Muneer A. 2008. *The Pakistan Lawyer's Movement. An unfinished agenda. Karachi: Pakistan Law House*.