Christopher Kullenberg

The Social Impact of IT: Surveillance and Resistance in Present-Day Conflicts

How can activists and engineers work together?

Since the 9/11 attacks the world has been challenged with intrusive legislation upon civil liberties and increased use of surveillance technologies. As this development is proceeding rapidly, both from a legal point of view and the technological side, it takes more than parliamentary politics to pursue a democratic and open discussion about these matters. This is where the civil society, or rather the civil societies, need to collaborate. Thus, I will propose that engineers, software-programmers and people in the private sector of Information Technology could co-operate with activists, human-rights organisations and citizen-journalists in a very productive manner. I will also give tangible examples on how such activities have been pursued in Sweden during a controversy on the role of signals intelligence.

Surveillance and War

Issues that keep arising in the backwaters of the "wars" on terrorism, drugs, and trafficking are often complex and require technical and legal expertise, not only to be understood, but more importantly, to be taken seriously in the public debate and by the media. In order to avoid that laws are passed without a proper debate or that technologies are implemented as merely technical solutions, I will propose that criticism could have a positive task in building a collaborative informational infrastructure, an effective media strategy, and other innovations.

Let me give an example from Sweden. During 2008, a law was passed which allowed the government to pursue extensive signals intelligence on the Internet. It was termed the "FRA-law" in the press, since the authority responsible for signals intelligence is called Försvarets Radioanstalt [1], which is the equivalent to the NSA in the United States, or the BND in Germany.

The FRA was previously only allowed to search and intercept radio traffic, but this new law would allow the authority to intercept all Internet traffic, by monitoring so-called "co-operation points" at the Internet Service Providers. By copying all the information passing through the cables, the FRA will be able to extract traffic-data from the multitude of data, both domestic and international. Consequently, a mode of operation which was developed in the context of the post-war arms race will be transferred to the Internet as this law is effectuated during 2009. However, the Internet is largely used by private and corporate communication, rather than military information, a fact that raises questions concerning privacy, integrity and the rights to private communication.

I will argue that if it were not for the active formation of a public, this law would have been passed without resistance or criticism. In order to understand how this works, the notion of a "public" is borrowed from the philosopher John Dewey, who explicitly stresses the importance of communication: "But participation in activities and sharing in results are additive concerns. They demand communication as a prerequisite. /…/ Communication of the results of social inquiry is the same thing as the formation of public opinion." [2]

Crucial to the formation of a participatory public issue, and to allow it to build political pressure, is the free flow of information in the sense that it operates without restrictions, something which is very different compared to traditional theories of mass-communication. This is where the Internet has a very interesting potential since its architecture, at least ideally, promotes participation, sharing and communication, which is precisely what Dewey is asking for. However, it seems that this free flow can not be guaranteed by the Internet alone, since the same abilities can be used for intrusive surveillance.

Panspectric surveillance

How are we then to conceive of contemporary technologies of surveillance? One way is to ask how technologies are used throughout society, by analysing their performances and abilities in socio-technical assemblages.

Digital technologies, besides sharing certain properties in hardware such as microprocessors, electricity-based operations and abilities to process instructions and algorithms, usually share many networked, or social effects. The Internet as an assemblage of computers, routers, switches and all kinds of IP-based technologies, such as mobile devices and satellites, shapes emergent forms of effectuation. For example file-sharing, voice-transmission, e-mails etc. are all dependent on interconnectivity. Also, they operate on the potentiality of decentralisation and read-write capacities, and on the ability to transfer the analogue world to a digital realm, which we see in the digitalisation of images, sounds, and even in the keystrokes of a keyboard.

There is however a critical paradox built into our mundane technologies. We may use digital cameras on our holiday trips and post the images on a blog, but we may also use the same capacities for an IP-based surveillance camera. The present day technologies are thus at the same time what may liberate sounds, texts, images and videos from their "material imprisonment" and geographical spatiality, while they simultaneously make possible for what is called panspectric surveillance [3].

The concept of panspectrocism comes from philosopher Manuel DeLanda, who situates the origin of these technologies in war. It is worthwhile to quote from his work *War in The Age of Intelligent Machines* (1991) in length: "There are many differences between the Panopticon and the Panspectron /…/ Instead of positioning some human bodies around a central sensor, a multiplicity of sensors is deployed around all bodies: its antenna farms, spy satellites and cable-traffic intercepts feed into its computers all the information that can be gathered. This is then processed through a series of "filters" or key-word watch lists. The Panspectron does not merely select certain bodies and certain (visual) data about them. Rather, it compiles information about all at the same time, using computers to select the segments of data relevant to its surveillance tasks [4]."

DeLanda thus argues that the technologies we face in contemporary debates on Internet surveillance, originate in a post-war setting which culminated during the cold war. Signals intelligence was born in a combination of radio interception, transferring analogue signals to digital information, and computers which calculated patterns, attached meta-data, and filtered out only the relevant pieces of information in a multiplicity of signals.

The birth of the panspectric technological framework, at least in an abstract sense, thus came from warfare. However, it was developed and refined during times when consumer technologies were not yet digital, and usually not even made for two-way communication (TV, press, radio).

What we see today is a complete change of orders. Signals intelligence performed by governments, such as the NSA, the FRA or the BND have entered a territory populated by ordinary citizens, rather than tanks, spy satellites and nuclear weapons.

Contemporary panspectric surveillance depends on the interconnectedness of sensors and computational methods such as data mining, sociograms and databases. Sensors include RFID-chips, digital CCTV-cameras, credit cards, mobile phones, internet surveillance etc., and they all have the ability to record an ever increasing part of our everyday lives. This is where we get close to the etymology of the words *pan-*, which means everything, and *spectrum* which is the entire range of detectable traces. The radical digitalisation of our societal functions and everyday lives, reconfigures and prolongs the range of surveillance. However, to make sense of this enormous abundance of data, methods of reducing complexity and finding relevant traces are needed. This is where the other pole of panspectrocism emerges; the need for supercomputers and advanced software and statistics.

The FRA has bought one of the fastest supercomputers in the world, and it is plugged directly into the central fibre-cables of the Swedish Internet Service Providers. They will consequently receive a copy of all traffic-data, and then process it in several steps in order to find patterns. The problem is, however, that traffic-data (which contains information about with whom, at what time, how frequently etc. we communicate) can say a great deal about you and your life. If we make social network analyses of the meta-data you give off during a normal day, the surveyor can probably find out who most of your friends are, and where you are most likely to be located. With more and more data, the surveyor is able to tell your religion, sexuality, political affiliation and consumer behaviour.

Citizen Journalism, Pirate Parties and Activists

We can make a tripartite division of activities that may challenge the increasing use of legal and technological means of mass surveillance; citizen journalism, pirate parties and activism. They may sometimes resonate in the same direction, towards a clear goal, but their basic properties and relations are essentially heterogeneous.

Issues, such as the FRA-law, can only stir up reactions and become "issues proper" if, following Dewey, there is communication between actors allowing them to react to what is imposed on them. It has been said that the case of the FRA-law was the first time in Swedish history that traditional newspapers lagged the blogosphere, and for the centre-conservative government the force of citizen journalism came as quite a surprise.

The blogosphere displayed a few interesting abilities by cooperating and sharing knowledge. One important aspect of raising issues, needed to be accounted for in this case, is speed. Paul Virilio argues in his book *Speed and Politics*, that: "If speed thus appears as the essential fall out of styles of conflicts and cataclysms, the current *arms race* is in fact only *the arming of the race* toward the end of the world as a distance, in other words as a field of action." [5]

Speed turns distance into action, and citizen journalism has a higher velocity than the traditional media, being dependent on printing presses, paid and professional journalists, or hierarchical organisations. During the passing of the FRA-law, the only ones being able to read legal documents, do proper research, and have a constructive discussion, were bloggers. In this case (and I do not want to generalise this observation to be valid for „the media" in general) we may say that the allocation of resources was much more efficient than that of large media corporations.

The critical task for the blogosphere in making a successful attempt at stopping this law is knowledge production. Surveillance technologies and intrusive legislations are complex matters which are often secretive in character. Signals intelligence is maybe an extreme case, since details about methods and search criteria is necessarily kept away from the public.

The first step in the case of the FRA was ontopolitical, in the sense that there was (and still is) a struggle to define whether signals intelligence is mass-surveillance, which would be a disaster for integrity, or simply a means to target very few „enemies of society" (terrorists). Bloggers analysed legal documents and government white papers, as a kind of swarm intelligence, and could argue convincingly that they entailed many legal exceptions for the FRA in registering political opinions, sexual orientation or religious background. The counter-argument from advocates of the law did not convince the bloggers, and the traditional media started covering the issue extensively. During the summer of 2008, there were articles in the newspaper almost every day for months, and many bloggers wrote extensively in both arenas.

From a technical point of view, the struggle was indeed one of definitions. It can be summarised in the question „How does the Internet really work?“ It may sound simple, but the understanding of the nature of technologies may be perceived of in many different ways. The legal documents in many ways still regard data transfers in cables as if they were basically the same as the aether waves that once gave birth to signals intelligence. Also, the advocates of the law stated that the FRA would not read the e-mails of ordinary citizens, and that it would be impossible to store all information that passed the fibre-cables on the net. This may be true or not, but it loses track of the question of mass-surveillance by only considering content-data, rather than the more intrusive kind of traffic-data [6], which the FRA has unlimited access to in practice [7].

Thus, in order to arrive at a citizen journalism which is able to form a strong public around an issue, both legal and technical expertise is needed, alongside social scientific and historical insights. If this is conveyed in a medium that is faster than traditional media, there is a chance of converting distance into action and making politics. Its effects on parliamentary legislation are however yet to be evaluated.

How an Engineer Can Be an Activist, and Activist Can Be Technical?

In digital rights there is a special dilemma in the relationship between legislation and technological systems. As technological innovations carry with them new social relations, make new communicational flows possible, and sometimes disrupt legislation [8] forcefully, I would argue that we need more than a "legalist approach" in understanding our contemporary situation.

The legalist approach to technological regulation may be understood as an idealist position, where we grant the rights and obligations to certain actors. For example file-sharing of copyrighted material is illegal in most countries, and we usually try to prevent the police, the homeland security agencies and several other governmental bodies to take away or override civil liberties. The legalist approach is thus a vision of rules that need to be obeyed. However, this approach is very limited in scope, and may work in a faulty manner as we try to open up the conflicts and constellations inherent to surveillance.

The other position we may call a performative approach, or along the reasoning of Rasmus Fleischer [9], a materialist way of understanding what technologies do in our everyday lives. Instead of asking what you are allowed to do with technologies, the performative perspective asks for what human-technologial assemblages are able to do. You are not allowed to share copyrighted material, but a computer and an internet connection make you able to do it, and this is why a substantive amount of the national internet traffic in Sweden consists of precisely this kind of files.

Anti-surveillance demonstration, 2008
(Photo by Andreas Käiväräinen)

With surveillance, we are running the risk that the surveyor may actually be doing what the harmless "pirate" is doing to copyrighted music or video. If there are systems enabling mass surveillance, we may similarly replace the violation of copyright into the violation of human rights. As mentioned earlier, we give the FRA the technological abilities to record all traffic data on the Internet, but not necessarily the legal means to use them freely.

No matter what your views are on file-sharing, we may still conclude that the Internet is changing the way we consume, share and even produce music. The disruption comes from technology, rather than a legalist process constructed in alignment with certain rights and duties. The materialist approach instructs us to regard such phenomena from parameters of technological analysis; The increase in bandwidth, storage capacity and the interconnected structure of the Internet enable simultaneously the massive flows of information and the tremendous, and necessary, generation of traffic-data. This data is however the core of panspectric surveillance.

Christopher Kullenberg

Christopher Kullenberg is a PhD-candidate in Theory of Science at University of Gothenburg. His main research concerns the co-production of the social sciences and social change. He is also writing frequently on the role of surveillance and social order, and is the editor of the Resistance Studies Magazine, rsmag.org. (christopher.kullenberg@gmail.com)

To conclude, we may say that securing legal rights does not suffice, but digital activism must necessarily be technical in character. It must affirm a materialist vision, which follows the flows of technologically enabled potentialities throughout society, and thus pushes the traditional front line of the legalist approach even further forwards, to where it hinges on the same level as the innovation, implementation and development of technological systems.

Engineers posses a certain kind of expertise, not only in their particular field, but in a more general way as it comes to understanding technological systems and their potentialities. French sociologist Michel Callon proposed in a 1986 article [10] that engineers were actually better sociologists than sociologists themselves, since the constructions and inventions of technological systems required a social analysis equal to the technical. Without knowing how to analyse social relations, you cannot change them and configure them according to you innovations.

However, there is a common view among certain engineers that their tasks do not stretch beyond finding mere technical solutions to particular problems. They distinguish between a technical problem and a social or legal one, and I must thus argue that such a conception is counter-productive.

Let me summarise the consequences in a few general sentences:

1. Activism and public debate must take place at the deployment of technological systems before they become mundane or their social disruption is forgotten in history.

2. Engineers, lawyers, activists and users can contribute to an open and critical debate if they co-operate, and may resolve issues on integrity on a practical level (e.g. encryption software, routing of messages, etc.) when forming heterogeneous constellations.

3. A performative approach may ensure civil liberties in a more rigorous fashion than a legalist understanding.

The Internet(s) – Democratic Spaces or Mine Fields for Panspectric Surveillance?

As there seems to be a general tendency towards more surveillance, not only in the EU member states but globally, it is easy to become absorbed with pessimism. Shaping publics does not seem to be enough, and turns into a democratic dilemma, especially in places where civil society is less likely to assemble. Technological activism, such as encryption and routing, may be effective, but could also be accused of denying the idea of a collective social and legal project.

I have argued not only that such an opposition is unproductive, but also that it is analytically false in its division of social and technological phenomenon. An issue may be formed around rights and parliamentary processes in the same fashion, as it takes an encryption protocol or a piece of hardware as its object. This "hacker attitude" [11] towards the politics of emerging technologies is maybe best expressed in the works of the French activist group *La Quadrature du Net*, who argue [12] that law is code, and if there are errors in it, activists should start "patching" them, instead of merely protesting towards them.

As all of these processes more or less take place on the Internet, simultaneously they are *about* the Internet, the expression of "reclaiming the streets" seems quite obsolete. Instead we should maybe say that reclaiming the cables, routers and lines of code would be the crucial task for a vibrant politics of the Internet(s).

Notes

[1] The official name in English is the National Defence Radio Establishment (see www.fra.se).

[2] Dewey, John (1998) The Essential Dewey: Volume 1: Pragmatism, Education, Democracy, Indiana University Press, p. 296, 304

[3] See www.panspectrocism.org

[4] DeLanda, Manuel (1991) War in the Age of Intelligent Machines, New York: Zone, p. 206

[5] Virilio, Paul (2006) Speed and politics. Los Angeles; Semiotext(e), 152, italics in original.

[6] This was uncovered in the largest Swedish daily Dagens Nyheter on September 3rd 2008. An English translation is availiable at: klamberg.blogspot.com/2008/10/fra-law-sleepwalking-into-surveillance.html

[7] As of early 2009, the original law which was passed in June 2008 is effective. However, there is currently a proposal to add special courts to increase control over the FRA. The role of the traffic-data is still not altered, and the FRA will start connecting physically to the Internet Service Providers in October 2009.

[8] Klang, Mathias (2006) Disruptive Technology: Effects of Technology Regulation on Democracy, Doctoral Dissertation, University of Göteborg.

[9] Fleischer, Rasmus (2008) En lektion i nätpolitik, Svenska Dagbladet, 2008-09-16.

[10] Callon, Michel (1987) Society in the Making: The Study of Technology as a Tool for Sociological Analysis. Pp. 83-103 in The Social Construction of Technical Systems: New Directions in the Sociology and History of Technology, edited by W. E. Bijker et. al. London: MIT Press.

[11] See also: Palmås, Karl & von Busch, Otto (2006) Abstract Hacktivism – The Making of a Hacker Culture, London: Mute Publishing Ltd.

[12] Zimmermann, Jérémy (2008) Presentation at the 25C3 congress in Berlin, 2008-12-30.