The Trust Situation

Why Data Protection Doesn't Protect Much

Dr. phil. des. Sandro Gaycken
University of Stuttgart
sandro.gaycken@philo.uni-stuttgart.de

Abstract:
Informational self-determination is an important ground for individual and societal notions of freedom. It relies on what we know about those surveilling us. However, as surveillance has become too huge a phenomenon to be "known" in any substantial sense anymore, generating informational self-determination has be delegated to data protection, a judicial canon which is designed to provide us with secure knowledge, at least in principle. But as data protection itself has grown a complicated topic, it has in fact only eroded our capacity to make any informed judgements. What we have to rely on in the end is hear-say knowledge and our trust regarding the involved agencies. And that's not good for our informational self-determination at all.

Exciting Times

Surveillancewise, we sure live in exciting times. Especially in Germany. We have warmongering ministers of the interior, suspecting terrorists and child molesters around every other corner. We have our police tuned in on their new paradigm of preemptive crime fighting (the „Neues Interventionsparadigma"). We have the sensors-industry in a goldrush with loads of fancy new devices, mimicking every sense we have or don't have in a most precise manner. They're joined by the IT-industry spawning ever new routines to track their customers. And unsurprinsingly we have the natural conjunction of all these ideas. Mutually reinforcing, they produce a massive increase in technologically mediated surveillance with a preemptive character, surveilling everyone independently of any real suspicion. Hundreds of such devices are currently developed, lending themselves to all sorts of political, security or commercial interests.[1] They enable the police or abstract entities as the „state" or the „law" just as well as the „market" or the boss to watch us, record us, profile us and sort us in highly efficient ways, readying our virtual selves for further processing of whatever sort. A time to worry? Many say no. We might have increased our surveillance. But we are still far from any sort of orwellian dictatorship. Surveillance is in good democratic control by data protection. Anyone suggesting differently is just one of those overly activated activists, who circle frenetically around highly hypothetical or exceptional cases. And the same people saying this tend to add stuff like: „Come on" or „Get real". However, I have my doubts that we (the activists) just play something up here. Actually, I have a lot of doubts.

One argument for instance which I believe to be quite substantial is that, despite the fact that we are not having a dictatorship *right now*, we cannot give any sort of guarantee for this status to remain over the next, say, 50 years. We wouldn't have learned a bit from history if we would.[2] And if we cannot do this, then why should we develop sociotechnical instruments and organizational structures which are only of limited use in a democracy[3], but of optimal use for any dictator interested in eliminating even the mildest type of hypothetical opposition in no time and with very little personnell? Preemptive surveillance technologies and the correlated social organizations have this kind of potential. The technologies enable their operators to recognise any sort of danger very early by what people do, how they communicate, how they inform themselves, how they move and interact. Thus, if you are dictator, simply re-define „danger" in whatever sense suits you and the machines and their operators will return you a list of all the „dangerous" people in no time.[4] In this

1 See http://www.securityresearchmap.de/ for an overview on what is done in Germany.
2 The Dutch philosopher Mark de Vries recently put very nicely: „the only thing we can learn from history is that we don't learn anything from history" (private communication).
3 About the criminological inefficiency, which is a very important point for the whole discussion, see for instance Albrecht (2008) or Gaycken (2009, forthcoming).
4 This has already be noted in the eighties by Gary T. Marx (1988) in his famous judgment on undercover police surveillance, but is equally valid for any sort of preemptive surveillance. And it definitely needs to be repeated.

sense, the sociotechnical structures of the new paradigm of preemptive crime fighting can have a strongly repressive, anti-democratic side-effect. This is not to say that they *produce* any dictatorship or that they *are* somewhat totalitarian. That wouldn't make much sense. But they do lend themselves very easily to any sort of totalitarian purpose and will maximize many of its effects. Thus, if society cannot control such a dangerous side-effect (or totalitarianism) at all times in the future and if that side-effect can turn devastingly against it at some point, it should be abolished in the present. Not the current freedom right now, but the preservation of our future freedom heavily depends on that. We need to replace the current paradigm of surveillance with a more moderate and sustainable kind. Ok, this is one of my earlier arguments.[5] I like repeating it as I deem it important for everyone to know. But it's actually not the one I want to sketch out here. The one I want to write about here makes a different point. While the first argument points to the fact, that preemptive surveillance cannot be controlled from getting into terribly wrong hands at some point in the future, this next argument will stress that surveillance already made us loose control in one very important respect.

The Death of Informational Self-Determination and an Unexpected Murderer

Now what is this thing which we have lost? I think it is our informational self-determination. It's dead. And what's even worse: one of its two murderers is the butler. Data protection has actually helped substantially in killing it. Let me tell you about this (philosophical) murder tale.

To start the story, we have to dive a little into the German formulation of the right of informational self-determination and try to find its essence. Don't worry, it's less tough (or boring) than it sounds. Informational self-determination states that we should always be able to fully know about anything that is known about us someplace else, so we do not have to suspect anything vicious lying around somewhere where we don't want that. Because – and this is already the essence of the informational self-determination – if we would have to suspect anything, however faint, we might decide to be cautious and adjust our behaviour in such a way that we better not do or say anything against anyone anymore. Just to be on the safe side. But being limited in such a way, we would not be very „free“ anymore, would we? We would no longer be able to speak our mind, to think for ourselves, to act for ourselves. And, conclusively, we could not be able to form a free and democratic society anymore. Such a society consists – per definition – of people who are free in this very aforementioned sense. Thus protecting the informational self-determination is an deeply important for anyone who wants to be free and it should be an innate and ongoing concern of any democratic state. The problem now is that this version of informational self-determination has been formulated in the mid-eighties. Back then, surveillance was limited and the gathering and storing of data was still a pretty hard thing to do and thus easily controllable. These days, things are different. Surveillance is becoming more and more omnipresent and data about us are constantly gathered, stored and processed without the slightest hassle. A change in degree, some might say, but in fact one which puts us into quite a different situation. With such complexity around us, how can we uphold our informational self-determination anymore? Surely noone will expect us to know every miniscule technological measure involved anymore, including all possible side-effects, every agent doing something with our data, intentionally or unintentionally, every institution with all its organizational routines and possible failures, and so on. If you still have a life to live, that is just utterly impossible. But then how can we fully know about anything that is known about us someplace else? The answer is: data protection. Data protection is a judicial corpus of rights which tries to warrant our informational self-determination by doing two things. First, it monitors all kinds of data collections and tries to restrain the collectors from gathering too many too individual data which might be able to spawn very personal informations.[6] Secondly, it tries to bring forth and maintain transparency by informing us about new surveillance measures and by enabling us to understand our particular rights to enforce disclosure on the data and informations gathered about

5 See for instance Gaycken (2008).

6 The distinction between data and information is the following: data is everything that is just bits and bytes, not read out and unable to say anything about anyone, information is everything that is put together in understandable, meaningful words (or images or whatever), able to say something about someone.

us. And that's how it works. Critical information are prevented, other data are noted and made accessible, so we can at least *in principle* be able to know everything known about us.

To Know or not to Know

So no problems anymore? No need to worry? Informational self-determination secured? I would say no. Because all data protection has put up is a huge and complicated apparatus of hypothetical „you-could-have-your-informational-self-determination-if-you-only-would-...". But in fact, noone does all those things data protection suggests. Noone informs herself precisely about all the kinds of data collected, all the agents and institutions involved, all the technologies and organizational structures. Noone understands those numerous rights of data protection in any sufficient detail, let alone enforces them with time and money against the myriads of surveillers we meet every day. Most people haven't even understood what data protection is in general or what it does.[7] Instead, what most lay people know about the current state of affairs is this: Everyone with money and power can surveill me almost constantly. There is some thing called data protection, but that's all lawyers, bosses and politicians again, complicated judicial stuff noone understands or takes the pain to get into. Period. This particular and certainly widely shared perception is the reality of how people meet the situation. Lawyers and scientists will now say: „It doesn't have to be like that. I *can* know everything". But that's exactly the point: *you* can. The average guy can not. Lay people instead *have to* rely on the *public* perception of surveillance and of data protection, not on the professional. And this public perception is the relevant and the only relevant ontology for the information self-determination. We can see that immediately. If we do not directly and precisely *know* everything about surveillance (in a scientific, professional sense of knowing), then what we *assume and suspect* about surveillance is the decisive element. It's the only way how we can judge the situation. And how are such assumptions and suspicions built? They are built by the public perception. By what we already believe about the involved actors and by some prominent cases coming to our ears through the media. Thus data protection has actually built us an illusion of knowledge where there actually is none. And it has done so – given the aim of generating secure knowledge for everyone and concludingly mostly for lay people – in the exact counterintuitive way: by adding more complex things to know.

Informational Mood-Dependent-Uncertainty

This plunges us into chaos. The bad kind of chaos, to be sure. Because as the average non-expert has to rely on the public perception and as that is mostly not very precise and informative on details, any following judgement has to be made in rather substantial informational uncertainty. This is the situation technical complexity *and* complex data protection laws and procedures have put us in. And it's a rather troublesome situation. It's not just that people will not have all the information needed for an informed consent. Much worse is in fact the psychological mechanism that how people relate to imprecise information and how they use it in actual judgements is quite angled. Tversky and Kahnemann have shown this long time ago and it's a well-known fact by now.[8] Hear-say-knowledge is not just knowledge. You pick what you like and forget or deny what you don't like and you rather believe people you trust than people you don't trust. So what you know (or what you think you can know in principle) multidimensionally depends directly on the prior opinion you have about the involved agencies, the confidence you have in them. Such a subjective and colorful „trust situation" is the real ground of any scarcely informed decision-making. For informational self-determination, this can immediately be shown to be generally bad. Because trusting those involved on either side of surveillance is asking quite something. To feel entirely secure and safe, to think and behave freely in this exceedingly surveilled world, people have to trust the state, the police, those in power, the secret services, the tax agencies, the banks, the big companies, the rich-and-richer or – in less

7 Funny story one researcher from the center for data protection in Kiel told me: He went on a tour in some company and was asked by the guide what he does for a living. He answers: „I do data protection". The guide answers, surprised: „Oh! That still exists?"

8 See the landmark book by Tversky/Kahnemann (1982).

institutional terms – lawyers, politicians, state authorities, salesmen and bosses. It is immediately clear that this is not exactely any sort of „most-trusted"-list. Quite the contrary. The informational self-determination of average lay people in fact depends on how trustworthy they consider a number of institutions and people which are commonly considered somewhat shady. Surely not by all people, maybe in all generality not even by the majority. But certainly by a huge part of the population and especially by those in difficult situations or with little access to knowledge in the first place, in other words: the socially weaker. And even for those who might still have full faith in all the agencies just mentioned, any sense of „real" informational self-determination must honestly be given up. All we really have is something like an „informational mood-dependent-uncertainty". And that is – to end the tale – why informational self-determination can be considered dead and partially murdered by data protection. Its successor, the informational mood-dependent-uncertainy, on the other hand is a very subjective, little rational and fragile little thingy, easily disturbed and not at all able to carry the heavy burden laid upon its weak and meager shoulders: our freedom.

A Really Real Concern

This is not just a hypothetical thing out of the brain of a philosopher. A number of already existing examples can be cited. People in need of aid such as troubled families or drug addicts already stop seeking such aid as they fear they might be identified and be observed closely henceforth, with ensuing disadvantages in other situations. Informants of the press remain silent as they cannot rely on their anonymity anymore, knowing that this might just not be guaranteed anymore. In Germany, we just had the Telekom scandal shaking that particular trust situation deeply and certainly for some time into the future, hindering the free press substantially in fulfilling its mission. The message many people got from this is that those „big guys" (and – by typefying extension – *any* „big guys") do not play by the rules anyway. They do what they want. So how can any informant to the press trust data protection to protect him in the first place? The same applies to many attestors or accused in court cases. They fear telling details of their cases to their lawyers as they fear that their lawyers might be wiretapped too. Thus many social arrangements needed in a just and democratic society or arranged in solidarity start to crumble. But do we have the right to exclude people in such situations from „felt freedom", from our free community? Are we ourselves free from this sort of exclusion? Maybe tomorrow someone *we* have to worry about might be interested in something we would rather see protected? Considering this, there are only two options. Either the technologies themselves have to be abolished again. Or we should be honest about the consequences, abolish – aloud and publicly – the whole idea of informational self-determination and say good-bye to freedom for all those who do not boast of confidence into lawyers, politicians and rich and powerful people in general.

References

Albrecht, H.-J. (2008): Kosten und Nutzen technisierter Überwachung. In: 1984.exe. Gesellschaftliche, politische und juristische Aspekte moderner Überwachungstechnologien. Hrsg. S. Gaycken, C. Kurz. transcript Verlag, Bielefeld.

Gaycken, S. (2008): Was habe ich eigentlich zu verbergen? In: Datenschleuder 92, Berlin 2008.

Gaycken, S. (2009, forthcoming): Rhetorik und Realität der Überwachung. In: Kontrollverluste. Interventionen gegen Überwachung. Hrsg. von Leipziger Kamera. Initiative gegen Überwachung, Münster.

Marx, G.T. (1988): Undercover. Police Surveillance in America. Berkeley.

Kahneman, *D., Slovic, P., & Tversky, A. (1982)*. Judgment under uncertainty: Heuristics and biases. New York.