Big Data Power

What to expect from mass surveillance

Nils Carqueville, Daniel Murfet

January 2014

At the beginning of the summer of 2013, Edward Snowden revealed the existence of secret mass surveillance programmes in the United States and elsewhere around the world. In the wake of the revelations there has been a public debate, with governments defending the programmes on the grounds that they are necessary for national security. In return many groups, ranging from civil rights organisations to ad-hoc coalitions of concerned writers, academics, politicians and other policymakers, have argued that these programmes represent a fundamental threat to democracy and must be halted or at the very least severely curtailed.

Where does this leave us, as individual citizens of our respective nations? Even after many hours reading the relevant articles it can be difficult to assimilate all the material, and from there to form a judgement about where reasonable use of state power ends and where dangerous abuse begins. On this question there is rational disagreement which cannot be dismissed as either the raving of attention-seeking paranoids or the gravelly booming of cheerleaders for totalitarianism.

With this in mind, our first intention in this essay is to briefly survey what is known about the mass surveillance programmes and why those advocating them believe they are necessary. The second and main part of the essay examines these claims of necessity, and lays out the present and future dangers inherent to mass surveillance.

Our contribution to the broader discussion is to stress how the problem goes beyond simply an invasion of privacy. In our view the real danger is the emergence of a radical new kind of power, and its potential for abuse. This power arises from the combination of two profound trends: the explosion of data generated by our digitally connected lives, and the growing understanding of how to extract knowledge from this data via clever software. The combination goes under the name of "Big Data".

Big Data is a potent source of power, if you happen to know who everyone is talking to, where they are, what they write in their emails and what websites they visit. This is information that the United States National Security Agency is now collecting on hundreds of millions of people. Unwarranted and untargeted programmes of bulk data collection of this kind are what we mean by "mass surveillance".[1] This data, combined with software which can mine it for knowledge, represents a new "Big Data Power" in the hands of our governments, and everybody else with access to it.

To be fair, we do not know that this new power is being seriously abused. But to wait until after such abuse is found before debating its legitimacy is an absurd standard that we do not apply to any other kind of state power. The power of the police or the military is supposed to be constrained to that which is necessary for them to serve their purpose; not because we think every policeman or soldier is unworthy of our trust, but because human institutions are imperfect, power corrupts, and all unchecked centralised power tends to be abused eventually.

Mass surveillance in a nutshell

There have always been surveillance programmes: a familiar example is wiretapping of phones, used in many criminal investigations. But until the Snowden leaks we did not know for sure that Western[2] governments are engaged in mass surveillance of their own citizens, that is, the collection and analysis of the private communications of hundreds of millions of

people not suspected of any crime. This mass surveillance takes place as part of the activities of signal intelligence agencies like the US National Security Agency (NSA) and the UK's Government Communications Headquarters (GCHQ). Thanks to recent leaks we know more about the operations of these two agencies in particular, and so in the following we often refer to them explicitly, but keep in mind that the mass surveillance club also boasts members from many other nations including France, Germany, and Sweden. This is a global phenomenon, not only an American or British one.

The organisations making up the mass surveillance club have their historical origin in cracking communication codes during the two world wars. This is still part of their activities, but they are now more broadly responsible for the worldwide collection and analysis of signal information – this includes phone calls, emails, and in general any information flowing over the Internet – for the purposes of foreign intelligence, for example knowing what other nations are up to, or what terrorists are planning. As our economies and militaries become increasingly digital and dependent on communication networks, the role of agencies like the NSA in national security will only become more central.

As part of this process, private communications of no relevance to foreign threats are collected, and therein lies the crux of the problem. But before discussing the problematic aspects, let us first survey the programmes themselves.[3]

The aspect of mass surveillance most discussed in the media in recent months is phone call metadata. The NSA collects the numbers involved in the phone calls, the time of the calls, and the location of both parties at the time of the call, for the approximately 100 million customers of Verizon. There is no reason to believe that Verizon is exceptional but at this time we have no explicit confirmation that this data is collected from other carriers.[4] Even when a phone call is not being made, cell phones maintain their connection to the network, and this requires switching between towers as we move around. Taken together the records over time of which cell phone tower our phones are connected to provides a digital "path of breadcrumbs"[5] which is stored by the operators of the cell phone networks. These records – more than five billion daily, from around the world – are collected by the NSA[6] and analysed by software to determine relationships, for example by looking for pairs of people spending time in the same place.[7]

This is a lot of data. But it is only a drop in the ocean compared to the collection of Internet communications. As far as they are able, the NSA together with GCHQ is collecting all of our emails, Internet browsing history and instant messaging chats.[8] We do not know the precise extent, but it is vast and probably close to total: for instance, we know that the data from popular services provided by Google, Facebook, Microsoft, Apple and Yahoo is being constantly siphoned off by the NSA. This sort of access is achieved in more than one way, and at worldwide scale: we know for example that GCHQ has tapped more than 200 of the transatlantic fibre-optic cables which carry Internet communications between America and Western Europe, and that it collects and analyses the huge quantity of data flowing over these cables.

The general philosophy was expressed by Keith Alexander, director of the NSA, in the form of a rhetorical question: "Why can't we collect all the signals, all the time?"[9] Speaking about Alexander, a former senior US intelligence official has answered this question for us:[10] "Rather than look for a single needle in the haystack, his approach was, 'Let's collect the whole haystack'." Needless to say, this is literally the definition of mass surveillance. Moreover, the Snowden revelations establish beyond any doubt that it has been going on for years.

This is a taste of the mass surveillance club's hunger for data. At this point it is not paranoid, but rather mundane and pedestrian, to say that if you can imagine data that might be interesting for them, they are probably collecting and analysing it or preparing to.

But why collect so much information?

The arguments in favour of mass surveillance

To explain from the government's point of view why the collection of all of this data is necessary, we will lay out the defense of mass surveillance based on public statements of intelligence community officials. In the name of intellectual honesty we will make the strongest argument we know how to make without lying.

The 9/11 attacks had a transformative effect on the landscape of US intelligence agencies. It became a focus for them to do a better job of "connecting the dots" in order to prevent future attacks. Since terrorists live among ordinary citizens, and use the same communication and transportation networks, these dots can be hard to see against the background. This is why the NSA believes that, in order to prevent

future attacks, it must collect all communications in order to find the relevant pieces of data and understand the links between them.[11]

This justification can be expanded in two directions. The first is that mass surveillance is a necessary reaction to the possibility of *forum shopping*: since terrorists can choose between many different channels of communication, they will naturally prefer the channels that they believe are not subject to surveillance. It follows that the only effective surveillance is total surveillance, across all forms of communication: instant messaging, email, phone calls, Facebook chats, etc. The surveillance must also be geographically total: there is no point surveilling only American Internet giants if terrorists can use email providers in Germany. In the words of the Director of National Intelligence James Clapper, intelligence agencies do not want to "give the adversaries, the terrorists, the prerogative of shopping around for providers that aren't covered."[12]

The second argument is that *information needs context*. If a known terrorist is talking to Bob on the phone, this information is much more useful if you know who else Bob is talking to, where he lives, and what his movements are for the last few months. Similarly, a single email or Internet browsing session is only fully meaningful when taken in the context of other emails and other browsing sessions. Since in advance it is impossible to know which communications are important for national security, and therefore which context you need to provide those important communications with meaning, the only solution is to get your hands on everything, everywhere and all the time.

The dangers of mass surveillance

The dangers of mass surveillance come in three groups, which we shall organise under the three headings privacy, power, and psyche. Privacy includes the right and ability to decide oneself whom to let into which layers of the sphere of one's personal affairs. We will argue that each of us stands to lose tremendously if we become transparent and stripped of the power to decide whom to share our secrets with.

The second category of threats from mass surveillance goes beyond the individual and is vastly more dangerous. Only a few years ago, intelligence agencies and private companies would have drowned in the oceans of data that are collected today. But very recently computer technology has made enormous jumps – changing everything. Practically overnight we have arrived in the age of Big Data, where it is not only possible to collect and store unprecedented amounts of data, but where a multitude of precise correlations of virtually every aspect of life can be extracted from it. In a word, vast amounts of *data* are converted to immense quantities of *knowledge*. Never before in human history has there been something remotely comparable to this ability (which is one of the reasons why it is difficult for us to judge its true scope and relevance). But knowledge is *power*. Big Data Power is a magnificent and qualitatively new kind of power – with numerous applications, but no less prone to compromise and corrupt one's character than other kinds of power. It is extreme and unprecedented, and in the hands of few it has catastrophic potential for manipulation and oppression.

The third danger we will discuss focusses again on us as individuals. It is less tangible, but simultaneously it strikes much deeper than the more direct violations of personal privacy. The expectation or knowledge of being constantly under surveillance, and subject to judgement of mighty powers makes us timid and colourless. If there are not even niches left to evade the all-seeing, prying eyes of mass surveillance, the pressure to blend into a depleted, grey mass becomes next to unbearable – even at the internal level. Mass surveillance takes our spark away, it reduces us to feeble shadows of ourselves.

Privacy

We now move on to a more detailed description of the above three dangers, starting with personal privacy. The last one or two decades have seen a steady erosion of our active appreciation of privacy, paralleling the rise of convenient online services and nearly ubiquitous access to computers of many shapes and sizes. Yet privacy is an inconspicuous pillar of a healthy democratic society.[13]

One can easily identify several professions whose success depends to a large degree on privacy. Among those which are also cornerstones of society are journalists, psychiatrists, priests, lawyers, and physicians. This is even clearer if we also take their sources, clients or patients into consideration – which means pretty much everybody. Without a high degree of confidentiality and trust, most of us would not want to discuss our deepest fears, urges or worries with a psychiatrist or priest; a legal case often involves delicate personal details, or depends crucially on control over relevant facts at the right time; we may be uncomfortable or even ashamed if others would

know details about some of our physical conditions or their treatments. Without privacy, we would be left on our own, without the essential support these and other professions can give us.

Other individuals who are particularly vulnerable to intrusion into their privacy are civil rights activists and people working for various non-profit organisations. It has historically been so,[14] and unfortunately it continues[15] to be the case that some of those in power use every piece of information at their disposal to compromise and diminish their political opponents. Even if the latter never even got a parking ticket and lead exemplary moral lives, we all know that the truth can easily be distorted and misrepresented, say by hiding relevant facts or context and by using suggestive language, to make it appear obnoxious, illegal or amoral. Obviously the more data is available the easier and the more effective such a cowardly and unfair undertaking becomes.

Not only the government and its agencies are in a position to abuse data and knowledge in the way just described. Everyone with the appropriate access can choose to blackmail or attack political activists or NGOs. This may include big companies[16] or individuals[17] working for the government or relevant companies that store sensitive information. Edward Snowden and those he shared his documents with have wielded this power in an exemplarily cautious and responsible way – disclosing information of immense public interest without endangering a single individual. But not everyone with skill and opportunity will adhere to the same high moral standards: technically versed employees of the government, its contractors or individual hackers may sell the information to someone who wants to compromise a political opponent or movement. In the world of Big Data, 'Black Snowdens' are bound to strike terror into people's hearts.[18]

Of course aggression and petty motivations are widespread ails, and there is no reason that Big Data will only be abused to target individuals engaged in political processes.[19] Personal revenge, envy or mere financial interests may lead someone to attack *you* – whether by hacking into databases themselves, or, much more likely, by buying your personal information legally[20] or illegally from a black market 'data dealer' (an occupation that will become even more lucrative). This someone would then know where you (or your phone) were when, what you used your credit card for, the contents of all your emails, all your Skype and phone calls, all your instant messenger sessions, and your complete browsing history. This is not information we want in the hands of someone who wishes us ill.

Power

We have already mentioned the sequence data–knowledge–power: the unfathomable amount of data that mass surveillance accumulates is subjected to modern data analysis which in turn extracts from it a vast ocean of correlations. This dwarves any kind of previous recorded knowledge by many orders of magnitude; the grand library of Alexandria or all the wikis in the world are but pebbles next to vast mountain ranges. In turn this enormous knowledge is a source of massive powers. We now move to consider some of the effects of this new type of power on society as a whole.

Before we discuss the consequences of mass surveillance from this angle, let us illustrate the potency of data–knowledge–power from a slightly different perspective. It has been widely reported[21] that a central role in the success of Obama's 2012 re-election campaign was played by a group of two or three dozen young physicists, computer and behavioural scientists. They took Big Data seriously, combining various databases and running clever algorithms to become the by far most accurate pollsters. Apart from the obvious advantages drawn from superior knowledge of trends, they also gave their team detailed instructions on how to successfully 'micro-target' millions of voters personally, and used their methods to improve general efficiency saving the campaign hundreds of millions of dollars. Clearly data was transformed into actual political power, helping to establish the current US presidency.[22]

If a few 20- and 30-somethings with access only to comparably tiny sources of data can have such an effect within just 16 months – what kind of power do those with billions of dollars, decades of experience, equipped with the latest hard- and software, employing (tens of) thousands of Phds in mathematics and computer science? What if they can collect and analyse a significant fraction of all the data on and off the Internet?

It is difficult to wrap one's head around such power, to fully grasp its meaning and potential; probably even many of those who now possess it are baffled by its extent. From the vantage of those who wield this power countless trends and developments in political and economical affairs and society at large will be transparent. It becomes possible to predict parts of the future we have no intuition for at all. In ancient times such insight and the power it brings would have appeared to us as god-like, were we confronted

with its entirety. Such powers may be amassed with good intentions, be they to protect a country from serious threats, or to build a useful and innovative business. Even if we assume that by and large these powers are utilised responsibly in the present,[23] they are bound to unfold into great dangers in the rather near future, of which we shall outline two.

While undoubtedly marred with deficits, the political systems in place today in many countries let their citizens live with many of their liberties intact while they benefit from the services provided by a central government. Unfortunately there is no guarantee this will never change for the worse. In fact despite all healthy optimism a sober look at historical facts and human nature teaches us that history is not only a monotonous development towards harmony and progress. Even the official report of 'The President's Review Group on Intelligence and Communications Technologies' cautions:

> ... we cannot discount the risk, in light of the lessons of our own history, that at some point in the future, high-level government officials will decide that this massive database of extraordinarily sensitive private information is there for the plucking. Americans must never make the mistake of wholly "trusting" our public officials. As the Church Committee observed more than 35 years ago, when the capacity of government to collect massive amounts of data about individual Americans was still in its infancy, the "massive centralization of ... information creates a temptation to use it for improper purposes, threatens to 'chill' the exercise of First Amendment rights, and is inimical to the privacy of citizens."[24]

Bring to your mind some of the regimes in recent years, decades or centuries with whom you disagree the most, to put it mildly. Now imagine that they had detailed information about every citizen's past and current activities, that they had the technology to master and integrate all this data and even predict likely future activities. For everyone individually and for society as a whole. How much more could they have 'achieved'?[25] And how much of such tremendous powers do we want to establish and hand over to any future leaders and regimes, ready to be paired with massive physical power and control? Since relying on the benignity of all future potentates is naive, mass surveillance is a nightmare in the making.

Yet future regimes, however far or near, are not our only concern. We know that power has a tendency to blind and corrupt, and that a taste of something that is good and healthy in the right dosage can lead to an unquenchable hunger for much more.[26] These are two of the reasons why mass surveillance has already grown far out of proportion. But even if everyone involved in establishing and analysing mass surveillance were an incorruptible role model and driven only by the best of intentions – even in such a hypothetical situation there are still terrible risks.

One is terrorism, but not the kind whose opposition is used as the main argument in favour of mass surveillance. Terrorism is not limited to physical violence and devastation: a terrorist's heinous aim spreads terror on a large scale may be equally well or even better served by more subtle, more efficient methods. Every week there are new reports of governments' or big companies' databases being hacked or subject to leaks.[27] Centralised data can never be absolutely safe, a dedicated attacker with appropriate means will find a weak spot in nearly every system. So far we have been very lucky in that the worst abuses we have seen are of a purely monetary type, on a scale far from endangering how we live together in society. What are the odds that there is no more severe harm in store for us? How long before a determined terrorist group realises the potential of Big Data for their agenda?

We have argued that detailed, meant-to-be-private information can be used to silence, shame or blackmail individual people. But with access to the Big Data of mass surveillance, targeting millions of people simultaneously is virtually as feasible as targeting individuals – literally only keystrokes away. Imagine what a terrorist group can achieve by attacking, say, social cohesion, trust[28] and respect among citizens, if they know all our emails, chats and browser history. What if, for example, a version of Google Maps were distributed that featured overlays with detailed data on, say, infidelity or any other severe breach of trust? Mass surveillance is a weapon of mass destruction waiting to be picked up.

Psyche

We return to the individual. Someone living in a climate of mass surveillance suffers immeasureably more than the comparatively superficial violations of privacy that we discussed earlier. To paraphrase a succinct characterisation:[29] "a person is that which is exclusively theirs." What does this mean for us on a fundamental personal level if so many of our actions and relations – and by inference our inner

workings, plans and desires – become transparent to those in control of mass surveillance?

What is ultimately at stake is our freedom of thought, our identity, our sense of self-worth and inner riches. A person with a reasonable expectation that their every act and word will be recorded, assessed, and possibly punished – such a person is one who learns to truncate their actions and words at the source: in their own mind. There is a powerful incentive not to deviate from the norm, not to draw unnecessary attention of the omnipresent eyes, ears, and possibly fists. Instead unconscious instinct and rationalisations will lead us to avoid confrontation with, and the judgement of, Big Data Power: by anticipatory obedience, self-censorship and self-reduction. "Surveillance breeds conformity."[30] It alters us at our core, it cages and shrinks our very self. Mass surveillance is soul-crushing.

To thrive and develop healthily we need space – space to be, space to think, space to experiment and explore, space for trial and error, space to dream, indulge fantasies and produce ideas. A necessary condition for such space is a good dollop of freedom, lack of direct or indirect intrusion and interference. Pervasive surveillance leads to karmic disaster: we lose virility and creativity, which are traded for meekness and lowliness. This makes us hollow, dull and uninteresting – to ourselves, and to our actual and potential friends and partners.

Much of this (and much more) is hard-won insight of those who suffered previous generations of (low-tech) mass surveillance in various countries. A frequently cited example are the spine-chilling, suppressive activities of the Stasi in former Eastern Germany. The everyday horror and plight of its citizens have become one of the epitomes of the viciousness of mass surveillance. Yet despite its immensity this horror and plight pales against modern and near-future mass surveillance. Having an agent or informant, an actual human, actively spying on you makes this act personal; the feeling of brutal intrusion and violation is immediate. Today's mass surveillance is much less personal; it is done by impassible algorithms and machinery, sneakily hiding in everyday technology. But the fact that the act of spying is not performed by a person makes it no less of an intrusion and violation, in no way are its consequences more benign. To the contrary, it only adds an explosion in effectiveness: all the people in the world would not have been enough for the Stasi to accomplish what today's mass surveillance does!

Right balance

With the arguments for and against mass surveillance laid out as best we can in the present format, it is time to compare them. In many ways the ultimate question is which balance to strike between mass surveillance as a tool for national security, and as an enabler of utter totalitarianism. Everybody has to decide for themselves what the right balance is.[31] It is however safe to assume that if each of us were paired with an actual human agent who follows us into every public space, office, bedroom and bathroom, taking notes of all our activities, never forgetting anything, drawing all kinds of conclusions and constantly telling all his spying friends about them – it is safe to assume that in such a grotesque situation most of us would agree that we were far off the right balance.

We personally believe that while our current situation is not quite as absurd as the one just imagined, it is clear from our description that in real life we have already dipped our toes into a terrible post-Orwellian nightmare. It is high time to wake up and retreat to safer ground.

What to do?

Given the extent of mass surveillance already in place, firmly anchored into all our lives, it may seem impossible to avert its stupendous dangers. More than that, once nearly everybody believes that those in command of Big Data are close to omniscient and very powerful, control and oppression become so much easier. Hardly anybody will dare to deviate from the norm, and even the idea of resistance will seem remote. Speaking out against mass surveillance even involuntarily strengthens and develops this narrative!

But this must be only an incipient side effect, part of a necessary first step to seriously tackle mass surveillance. The burden of engaging this repugnant situation has been placed upon all of us. Yet it is not true that all is lost, that we stand entirely impotent and helpless before this overarching danger. We believe that it is hard but possible (and right!) to shrink Big Data Power back to a healthier size – the alternative is simply unacceptable.

One of the most important ways to act is open to each of us individually. Part of the good news is that a lot of the technology to hold the dangers of mass surveillance at bay is already available. Thanks to the hard work of a dedicated community of computer experts, strong encryption and anonymisation for emails, chats, telephony and many other applications is possible for everyone.[32] It is very simple:

if nearly everybody encrypts their communications and anonymises their private online activities, Big Data Power abuse is already stopped at the initial step of collecting usable data. Intelligence agencies could go back to focussing on actual suspects and targets.

Usability has improved enormously in the last couple of years and will undoubtedly continue to do so. Once encryption is properly set up on your desktop, laptop, tablet or phone everything works pretty much as easily as before. Initial configuration is only slightly more work, but when in doubt one can always ask a technically more versed friend, relative or neighbour for support – they will likely be very glad to help.

Another option for everyone lies in their role as voter, customer and citizen. While relying only on politics to solve the problem all by itself is overly optimistic, it must be part of a lasting solution. Important demands are to hold up and strengthen constitutional rights, to rein in pro-surveillance legislature like FISA or the Patriot Act, the disassociation of military and intelligence organisations, reduction of secret jurisdiction to a bare minimum, and the implementation of actual, potent parliamentary oversight – in every country. We can express our concerns and suggestions to politicians by writing letters, making phone calls,[33] or seeking direct personal meetings. Civil rights groups like the EFF, ACLU or CCC[34] are very good in this department, and they can use a lot of support. Furthermore, we can avoid companies and services with problematic privacy and data policies, or because their magnitude and ambition simply gives us the creeps.[35]

All of these actions have little to no effect if only a small minority engages in them. But once many of us embrace them they will make all the difference. Apart from the initial 'activation energy' necessary to change some of our habits and routines, these individual actions come at basically no cost at all (as is true of so many ethical changes). In this sense we have a chance to seriously curb mass surveillance for free!

Some of us are afforded additional ways to help avert the dangers of mass surveillance: Teachers, in particular professors in mathematics and computer science, can appeal to the conscience and responsibility of their students and potential future employees of intelligence agencies, their contractors or other likely Big Data abusers. Similarly, system administrators, software developers and hackers can use their expertise to educate the public and uncover wrongdoings should they come across them. Journalists can join those of their colleagues who already report seriously on mass surveillance issues. Artists can literally paint the picture of what mass surveillance does to the human soul, helping us to understand and internalise the less tangible dangers. Everyone who has friends in positions of power can tell them about the threats of mass surveillance and suggest using that position to help avert them.

Many avenues are open.

Conclusion

Mass surveillance is taking place. We have surveyed why governments believe it is necessary, and also the three main classes of dangers that we see growing out of it: the invasion of our privacy, Big Data Power and its abuse, and the subtle but profound tendency of mass surveillance to deaden our inner lives.

But there is good reason for hope. Ending rampant mass surveillance is in everybody's interest, and our opposition is a force which brings us together regardless of our other opinions on society. In this common ground lies a seed, the growth of which will help us overcome our own feelings of individual powerlessness. This growth can be fed by continuing to grapple with the concept and manifestations of mass surveillance, and to keep making it a topic of private and public discussion. Together, this is how we begin to defuse one of the greatest dangers of our times.

About the authors: Nils Carqueville is a professor in mathematical physics at the University of Vienna. Daniel Murfet is an assistant professor in mathematics at the University of Southern California.

Notes

[1] To be clear, we are exclusively discussing *mass* surveillance in this sense; targeted surveillance of individuals as part of traditional intelligence gathering is not a topic of this essay.

[2] Of course China and many other nations have been doing this for decades, and many suspected that it was also taking place in countries like the United States.

[3] All of these programmes were secret, and are known to us now only through interviews with Edward Snowden and the internal slides and documents he has leaked. Our statements are based mainly on these slides, together with context provided by articles authored by journalists who sometimes have access to internal sources to corrobate or elaborate the facts gleaned from these slides (which are obviously not written for an outside audience, and therefore often lack context). Some of these facts have later been "made official" by figures such as NSA director Keith Alexander, or the President's review group, but it would be distracting to make very explicit the chains of knowledge by which we know any particular fact. For a more comprehensive survey we refer to the following websites that try to keep up to date with all revelations from the Snowden documents: Wikipedia, IC off the Record, Cryptome, EFF.

[4]See *NSA collecting phone records of millions of Verizon customers daily*, Guardian, June 2013, and *C.I.A. Is Said to Pay AT&T for Call Data*, New York Times, November 2013.

[5]An illustrative example of what can be gleaned from mere cell phone metadata (collected over six months for just a single person) is the interactive map and text of *Betrayed by our own data, Zeit online, March 2011.*

[6]See *NSA tracking cellphone locations worldwide, Snowden documents show*, Washington Post, December 2013, and *New documents show how the NSA infers relationships based on mobile location data*, Washington Post, 2013.

[7]In 2010 and 2011 the NSA had a "test programme" to collect and analyse this information specifically for US calls, and it remains unclear to what extent this continues today, but this is a distraction: the larger FASCIA programme is known from leaked slides to have at least continued until 2012 when the slides were made. See *NSA had test project to collect data on Americans' cellphone locations, director says*, Washington Post, October 2013, and *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, New York Times, September 2013.

[8]Relevant code names are XKeyscore and Tempora. Part of this is the PRISM program, where the NSA makes formal requests for data to major American Internet companies such as Google. These requests are secret, and we do not know the extent of the data that is provided in this manner. But PRISM is less important than the data obtained by the NSA and GCHQ by infiltrating Big Data company networks like those of Google and Yahoo, or directly tapping fibre-optic cables and international data hubs to extract all Internet traffic indiscrimately, using the TURMOIL program among others.

[9]See *GCHQ taps fibre-optic cables for secret access to world's communications*, Guardian, June 2013.

[10]See *For NSA chief, terrorist threat drives passion to collect it all, observers say*, Washington Post, July 2013.

[11]The purpose of the NSA is not limited to counterterrorism, and it is probable that internally mass surveillance is defended on grounds which are wider than catching terrorists. However, given that this is the only argument so far put forward by NSA officials in their defense, it is the one we will stick to. But we want to be clear that another defense that can be anticipated, namely that mass surveillance is necessary, in some form or another, for defense against cyber attacks, is subject to the same considerations as terrorism in our view.

[12]See *NSA had test project to collect data on Americans cellphone locations, director says*, Washington Post, October 2013.

[13]In particular, privacy is much more than the comparably petty and inconsequential question of whom to share photos with on Facebook.

[14]Compare e. g. the New Jim Crow, or the case of Martin Luther King who received anonymous letters from the FBI that were intended to drive him into suicide.

[15]Compare e. g. Japan's new state secrets law: *Japan Passes Draconian Secrecy Bill Into Law: Journalists, Whistleblowers are now "terrorists"*, Japan Subculture Research Center, December 2013.

[16]See *The war on democracy*, Guardian, November 2013.

[17]See *What Surveillance Valley knows about you*, Pando-Daily, December 2013.

[18]See also *The Surveillance State Puts U.S. Elections at Risk of Manipulation*, The Atlantic, November 2013.

[19]See also *Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'*, Huffington Post, November 2013, and *LOVEINT: When NSA officers use their spying power on love interests*, Washington Post, August 2013.

[20]See e. g. *What Surveillance Valley knows about you*, Pando-Daily, December 2013, and *How Your Data Are Being Deeply Mined*, The New York Review of Books, January 2014.

[21]See *Google's Eric Schmidt Invests in Obama's Big Data Brains*, Business Week, May 2013.

[22]Needless to say that many of the group's analysts have since founded a thriving company called Civis Analytics (co-owned and financially backed by Google's Eric Schmidt), selling their expertise to other campaigns as well as private companies.

[23]Such veracity and good intentions are called into question by the degree of lies, evasions and schemes exhibited by senior spy coordinators. For example, James Clapper famously lied to the United States Senate Select Committee on Intelligence about the NSA's data collection on hundreds of millions of Americans, and Keith Alexander repeatedly made similar statements. Furthermore, official NSA statements are nearly exclusively about the comparably harmless bulk collection of phone metadata, attempting to make the much more extensive surveillance of virtually all Internet communications a non-topic by consistent omission. And in a disgusting attempt to establish a modern newspeak dialect, the word "surveillance" is claimed not to describe the automated collection, storage and analysis of data, but reserved exclusively to the act of a human agent actively examining the end result on a screen.

[24]See *Liberty and Security in a Changing World*, December 2013, page 116. Another relevant quote from this official report: "Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders."

[25]Larry Klayman's take on this is as follows: "If our Founding Fathers had lived in these times, and if King George III had had an NSA with that kind of technological capability, the Founding Fathers would have been picked up, arrested and executed before they ever got to Philadelphia to sign the Declaration of Independence."

[26]This is true of chocolate, but also in Big Data domains, compare e. g. toll collect systems in the UK or Germany, or recent legislation in Japan or Sweden, massively extending the reach of government and intelligence agencies.

[27]One of the most recent cases is the theft of up to 110 million payment card details and other personal data of customers of the US retailing company Target last December, see *For Target, the Breach Numbers Grow, New York Times, January 2014.*

[28]In the words of Nobel prize winner Joseph Stiglitz: "Trust is what makes contracts, plans and everyday transactions possible; it facilitates the democratic process, from voting to law creation, and is necessary for social stability. It is essential for our lives. It is trust, more than money, that makes the world go round."

[29]Attributed to Lord Cottenham in S. D. Warren's and L. D. Brandeis' essay *The Right to Privacy*, Harvard Law Review, V. IV, No. 5, 1890.

[30]See *Glenn Greenwald: What I've Learned*, Esquire, December 2013.

[31]Of course mass surveillance does not equal national security. For example, two recent studies conclude that dragnet surveillance played a minute role in counter-terrorism activities in the US, see *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, New America Foundation, January 2014, and

Connecting the Dots: Analysis of the Effectiveness of Bulk Phone Records Collection, Hoover Institution, January 2014.

[32]All emails and other files can be encrypted using Gnu Privacy Guard, also called GnuPG or GPG. There are convenient bundles like GPGTools or Gpg4win which make integration with Mac OS or Windows easy, but using it under Android, iOS and Linux is just as straightforward. Another important application deserving privacy is Internet telephony. Instead of using Skype or FaceTime to share all our conversations with Microsoft, Apple and various intelligence agencies, we can use off-the-record (OTR) encryption, for example with the cross-platform programme Jitsi. This and a lot more free and open privacy- and freedom-related software is listed and explained on the website prism-break.org; Bruce Schneier also offers good advice.

[33]Members of the US Congress can be reached via the website callcongressnow.org.

[34]Electronic Frontier Foundation, American Civil Liberties Union, Chaos Computer Club.

[35] Not only more traditional big players like Hewlett-Packard, IBM or Lockheed Martin are currently bidding for a $450 million cloud computing contract with the Defense Information Systems Agency, but also Big Data companies like Amazon, Google or Microsoft. Google has recently become part of military-industrial complex also in more direct ways, e. g. by aquiring robotics companies like Boston Dynamics which have multi-million dollar contracts with the Pentagon's Defense Advanced Research Projects Agency and other branches of the military. President Eisenhower's warnings have not forfeited any of their urgency: "The potential for the disastrous rise of misplaced power exists, and will persist. We must never let the weight of this combination endanger our liberties or democratic processes. We should take nothing for granted. Only an alert and knowledgeable citizenry can compel the proper meshing of the huge industrial and military machinery of defense with our peaceful methods and goals so that security and liberty may prosper together."