Towards A Clean Slate: Attempting to Preserve Civil Liberty in the Post-Snowden Age

Alexander von Gernler

Abstract: Wide adoption of mobile computing, smartphones, social networks and big data techniques have brought undoubtable advantages to society as such, as well as to its individuals. The downside of this diffusion of technology throughout society has already been well discussed. Single authors also pointed out the threats not only to the single individual, but to democratic society as a whole. However, suggestions or even practical approaches of how to mitigate these threats not only at the individual level (Folks, keep your virus scanner up to date all the time!), but for society itself, are rarely found up to this day.
There is no simple solution to this problem, of course. Particularly not a small one that can be carried out by a single peer group. Rather, we want to motivate that there are different approaches to the shared common goal of preserving civil liberty for many individual groups of society. In this article, we focus on a strategy for computer scientists on how to perform their part in the big picture, and try to motivate this by calling up on their professional ethics.

ACM CCS: Security and privacy → Human and societal aspects of security and privacy → Social aspects of security and privacy; Social and professional topics → Computing / technology policy → Surveillance

Keywords: Surveillance, Democracy, Open Hardware, Clean Slate

1 Introduction: The big picture viewed through the eyes of a practitioner

1.1 Resistance is futile

The wide-spread use of information technology has let the computer, or better yet, thousands of computing devices, take a central role in every person's life. Not only has the smartphone truly become the *personal wallet* as envisioned by Bill Gates [1] in 1995, but its offered possibilities are even bigger, and grow with every new app written by one of the hundred thousands of developers. The eagerness to adopt these new techniques and the nearly fanatic way of collecting data and being transparent (*quantified self*) that some users display as a flanking effect of these new media has also been criticized, for example by Schirrmacher or Han [2, 3].

But even people trying to live very basic and minimalistic *offline* lifestyles can no longer escape modern information technology, as it is contained in their car, their public transportation, their TV set (if any), their passport, or their supermarket's checkout counter, just to mention a few [5]. It has become such a profound and undeniable cultural technique that renouncing even these basic commodities in order to be *offline* would result in leading the life of a hermit. And even then, ironic enough, some hikers will probably stop by, take a photo of you and post it on Instagram.

Equipped with the commonplace knowledge that there is just no escape, another important question arises. It has at first been overlooked, but the Snowden revelations made it necessary for the average mind (not only for the people wearing tinfoil hats, that is[1]) to think about it: If those systems make our lives so much more desirable, comfortable, efficient and connected, so that everyone depends on them, then these systems are secure and trustworthy, right?

[1] Because *we* [8] knew it all along, of course!

1.2 The NSA attack

You may substitute *NSA* for every big governmental agency or big company that you like, because it will not make the following theses less or more true. The name is chosen because the tipping point that made it all so visible indeed was in the Snowden revelations [6]. They have then also been called the *NSA scandal* in mainstream (*NSA affair* in German) media, and reports about it have mostly been on smartphone X, undersea cable Y and mail interception project Z. This is true on the one hand, and on the other, it could not be further from the truth. Thus, we present two theses on the *NSA affair*:

1. The *NSA affair* is not an affair.
2. The *NSA affair* is not about technology or engineering. It is about nothing less than the question in which kind of society we want to live tomorrow.

Thesis (1) is easy to prove, which has been done by Lobo [7] already: An affair describes a matter of limited time, whereas the dragnet-like activities of government agencies against Internet communication have not been stopped since the Snowden revelations, but, we may safely assume, most likely increased. Lobo hence uses a more aggressive wording to lay emphasis on its still-ongoing character, speaking of the *NSA attack*.

Thesis (2) has been sufficiently discussed by Schaar, Greenwald, and others [5, 6, 3]. Their baseline message is that both the massive transparency created by careless or indifferent users who display information about themselves and the massive dragnet-like online surveillance pose serious threats to our democratic society. In this contribution, we want to take their arguments a little further and talk about possible consequences.

2 Democracy – what is it?

Great philosophers of all generations since the age of the Ancient Greek have produced a veritable amount of literature on democracy that we will not try to challenge here. There also seems to be a broad consensus in western culture that amongst human rights, clean water, an intact environment, the solution to the population and world energy problems, democracy is one of the key legacies that we want to pass on to the world that our children will live in.

This section is therefore about the necessary requirements for democracy to continue working in the digital age, from a computer scientist's point of view. Figure 1 shows an incomplete dependency graph that we have identified during our research. The upper part of the graph displays the basic and historical reqirements, whereas the lower part shows the additional requirements for a working democracy in the digital age. There are side branches missing that would address other areas of expertise or would leave the focus of this contribution.

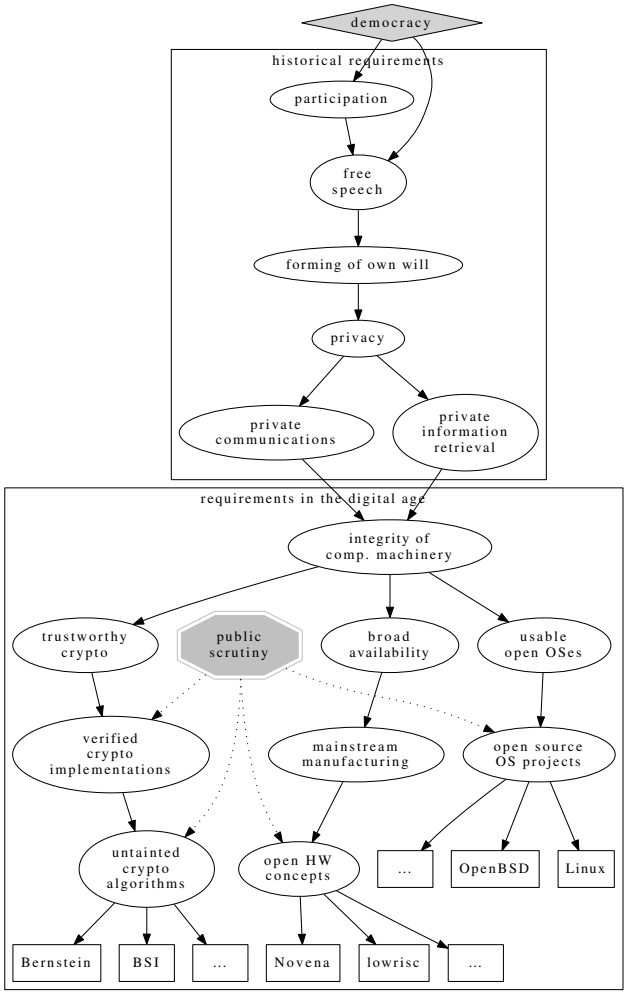

Figure 1: Dependency graph for democracy. Regular arrows: *depends on* relation; dotted arrows: influence.

But as far as this article is concerned, the graph should be sufficiently complete.

2.1 Historical Requirements

Greenwald and Schaar did not invent the wheel from scratch when they stated that for a working democracy, privacy comes automatically as a main prerequisite [6, 5] – it is merely a historical commonplace and can be a safely assumed dependency for the sake of this article. The short explanation is: Whenever an individual trying to form his free will is aware of being observed, he will stick to whatever he perceives as the current *socially acceptable answer* that fits best into the *major consensus narrative* [13], rather than expressing his innermost and truly conceived feelings about a given subject. The fear of punishment – both by the government or by society – plays an important role here. Since the uninfluenced forming of free will is essential for a working democracy, privacy is a necessary condition.

In the dependency graph, we added some intermediate steps for clarification and finer granularity, outlining Greenwald's argumentation, but privacy is basically one

non-negotiable feature required for democracy. Privacy covers both the retrieval of information itself (civilians informing themselves) as well as the discourse about it. While in earlier ages, an agora (e. g. market place) and some means of confidential messaging (e. g. sealed scrolls) might have sufficed, cultural techniques have vastly changed up to the 21st century. This leads to the bottom part of the dependency graph.

2.2 Requirements in the Digital Age

Because in the Digital Age, the vast majority of both communication and information retrieval is performed by electronic means, it is of crucial value that the platforms used to carry out these interactions can be considered trustworthy. Other requirements about transport of information or the server side are also needed, but not in the focus of this article. We discuss the end users' hardware here, because without a secure end point, all further discussion of this topic would be obsolete.

As the second subgraph in figure 1 shows, integrity of computational hardware can be divided in at least three main aspects: Trustworthy cryptography, broad availability of the platform and a trustworthy and usable operating system. For each one of the three main aspects,

1. there is at least one intermediate step on the path that allows for public scrutiny.
2. there are already working reference instances in the leaves of the graph available that can be used to build on.

The first fact is essential if the resulting platform is supposed to ever gain public acceptance: Only independent verifiability will create trust here.

The second fact is important with regard to feasibility: A trustworthy, open platform for the end user is possible – there are no obstacles in the way that could not be tackled! Of course, this does not yet create a viable business model that will supply us with said platform instantly and on big scale, but this is an ongoing task.

It is good to see that our approach also meets claims that the Federal Constitutional Court of Germany made in 2008 about the *basic right on confidentiality and integrity of IT systems* [12]. However, we must find that despite the court's verdict, the reality looks quite different at the moment: There is virtually no trustworthy platform out there that has production quality, is deployed out in big scale and is comprehensible to the end user. To be noted well, this applies to all of the platforms, not only the mobile ones. There is especially no trustworthy i386/amd64-compatible server, desktop or notebook available that could be purchased on a commodity scale. The *traditional* IBM-PC-derived platforms at the moment suffer direly from too much complexity and uncontrollable and well-exploitable add-ons like Intel AMT [16].

2.3 The way out

Figure 2: The Novena [11] Open Hardware Platform. (Picture taken from its project page at `crowdfunding.com`, assuming fair use)

Summing up, this approach would mean to start with a clean slate as proposed for example by Bogk in 2014 [10]. This was not an originally new idea, as Neumann and Watson [14] already adressed this in 2012, and a DARPA Program named CRASH [15] of unknown date points in the same direction. Both ideas, however, did not receive wide adaptation yet.

A more recent and very promising approach was done by Huang [11] on the platform `crowdfunding.org`: Figure 2 shows a picture of the Novena Open Hardware Platform [11] that is about to ship just at the time this article is being written. Another upcoming project is `lowrisc.org`, a non-profit organisation working closely with the University of Cambridge.

In our opinion, without a trustworthy foundation, all effort to create security on some application on the top of the stack is damned to be irrelevant. A trustworthy foundation in turn would mean control over and public scrutiny on a trustable stack comprised of the components mentioned above: Hardware, OS and Crypto.

3 Undeniable Responsibility

Han states that scientists nowadays often do not fully reflect the societal context of their knowledge [4]. We agree insofar as our own observations suggest that today, scientists are being forced to act as a manager for their research group or teaching chair, and, even worse, hop from one funding project to the next just in order to get their regular operational expenses (read: research team) funded. Cynically put, this allows them conduct their own research only in a time-efficient and streamlined manner, and bans ethical considerations to their spare time, making them become as much as a sideline nowadays.

However, not only since Dürrenmatt [17], we know that there is no such thing as context-less research. Saitta and Norton illustrate this principle by stating that *technology is neither good nor bad, nor is it neutral* [18]. Scientists therefore are (and have been) well advised to always consider the impact of their research on the real world.

With nothing less than the future of our society at stake, computer scientists of all disciplines, academics as well as practitioners should put aside their daily business for some time, and dedicate their efforts to one goal that we believe is necessary to share in common: The goal of a trustworthy and open hardware platform that allows us to do research, do business and live as free citizens in tomorrow's digital world.

4 Conclusion

Rescuing privacy and free speech in the Digital Age in the long run will take a lot of effort in many different places and topics [9]. It can not be carried out alone, or by a single group. However, computer scientists must recognize their responsibility for society in taking both a warning and a protecting role for their fellow citizens who do not posess the technological judgement that is needed for certain vital questions.

Literature

[1] Bill Gates. *The Road Ahead*. Viking Penguin, November 1995.

[2] Frank Schirrmacher. *EGO: Das Spiel des Lebens*. Verlag Karl Blessing, München, 2013.

[3] Byung-Chul Han. *Big Data: Dataismus und Nihilismus*. Zeit Online, September 2013.

[4] Byung-Chul Han. *Tut mir leid, aber das sind Tatsachen*. Zeit Online, May 2014.

[5] Peter Schaar. *Überwachung total. Wie wir in Zukunft unsere Daten schützen*. Aufbau Verlag, Berlin, 2014.

[6] Glenn Greenwald. *No Place To Hide. Edward Snowden, the NSA, and the U. S. Surveillance State*. Metropolitan Books Henry Holt and Company, New York, 2014.

[7] Sascha Lobo. *Rede zur Lage der Nation*. re:publica, Berlin, May 2014.

[8] Frank Rieger and Rop Gonggrijp. *We lost the war. Welcome to the world of tomorrow*. 22C3, Berlin, 2005.

[9] Frank Rieger. *Was tun? Vorschläge für Auswege aus der Überwachungsfalle*. fiffkon, Berlin, 2014.

[10] *SPD will Open-Source-Sicherheit staatlich unterstützen*. derStandard.at, April 16th 2014, visited on Mar 1st 2015.

[11] Andrew Huang. *Novena. Open Hardware and F/OSS-friendly computing platform*. http://www.kosagi.com/w/index.php?title=Novena_Main_Page, visited on Mar 1st, 2015.

[12] Federal Constituitonal Court of Germany. *Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274. Karlsruhe, 2008

[13] Bruce Sterling. *Zeitgeist*. 2000.

[14] Peter G. Neumann and Robert N. M. Watson. *CTSRD – Rethinking the hardware-software interface for security*. Joint research project. Cambridge, 2012. http://www.cl.cam.ac.uk/research/security/ctsrd/, visited on Mar 11, 2015.

[15] Darpa Innovation Office. *Clean-Slate Design of Resilient, Adaptive, Secure Hosts (CRASH)*. http://www.darpa.mil/Our_Work/I2O/Programs/Clean-slate_design_of_Resilient_Adaptive_Secure_Hosts_%28CRASH%29.a visited on Mar 11, 2015.

[16] Patrick Stewin. *Persistent, Stealthy, Remote-controlled Dedicated Hardware Malware*. Chaos Communication Congress. Berlin, 2013.

[17] Friedrich Dürrenmatt. *Die Physiker*. Diogenes Verlag, Neufassung 1980.

[18] Eleanor Saitta and Quinn Norton. *No Neutral Ground in a Burning World*. Chaos Communication Congress. Berlin, 2013.

Alexander von Gernler studied Computer Science at the University of Erlangen (Diplom 2005). He was committer in the OpenBSD project (2005-2010). He joined genua mbh in 2005, working there up to this date. His positions at genua include Software Developer, Scrum Master, Technical Ambassador and currently Head of Research and Project Development. Alexander von Gernler was granted the GI Junior Fellowship in 2014.

Address: genua mbh, Research and Project Development, Domagkstr. 7, 85551 Kirchheim bei München E-Mail: alexander_gernler@genua.de