The Future of Security and Privacy*

Bart Preneel

COSIC, an imec lab at KU Leuven, Dept. Electrical Engineering-ESAT
Kasteelpark Arenberg 10 Bus 2445, B-3001 Leuven, Belgium
bart.preneel@esat.kuleuven.be

Abstract. This paper attempts to identify the most important trends in information technologies and their impact on security and privacy. It considers developments such as the emergence of the Internet of Things, Big Data and edge computing. It analyzes how the digitalization has created new risks and has resulted in mass surveillance by nation states and corporations. It discusses the role of cryptography (the crypto wars) and the societal impact of active cyber attacks by nation states and specialized companies. Finally, it reflects on some technical approaches that society can take to maintain the balance of power between individuals, corporations and governments.

1 Technology Trends

The **Internet of Things (IoT)** is a network that connects the Internet of servers and clients with a huge number of objects in our environment, hereby expanding human-to-machine communications to machine-to-machine communications [10]. The IoT comprises embedded devices integrated into homes, office buildings, factories, vehicles, but also complete cities ("smart cities), and agricultural infrastructure. It will also include human-implanted devices. Current estimates indicate that by 2020 20 billion devices will be part of the IoT with growth to a hundred of billion or more in the next decade. This development has an enormous potential to improve the quality our lives, but brings major security and privacy risks. The security risks change in nature as they translate to safety risks, that is, human lives are at stake; privacy risks are exacerbated by the fact that it will be impossible to evade this infrastructure and by the integration within our bodies. Securing such a network is a huge technological challenge, in particular when we consider that higher security levels will be necessary than for the current Internet. The main challenge however is economical: research has pointed out market failures in security and privacy resulting in under-investment. The answer will have to come from regulation: the first laws are currently being enacted, but they are either too weak (California solution [1]) or they rely perhaps too much on certification (EU Cyber Act [2]). While certification is clearly part of the puzzle, there is a substantial gap between

* To appear in Proceedings Santa's Crypto Get-Together 2019, Prague, Czech Republic, 5-6 December 2019, Springer-Verlag, Lecture Notes in Computer Science.

the current approaches to certification (such as the Common Criteria) and the market need for cost-effective, agile and efficient certification methods.

Big Data is the trend to collect, store and process ever-larger quantities of digital data, characterized by high volume, variety and velocity [12]. This development is driven by the dropping cost of computation, communication and storage that has resulted in the emergence of both cloud computing and the IoT. Sophisticated analytics methods are being developed to identify trends and predict future developments; this includes deep learning that has automated complex tasks such as visual processing. Again, the potential benefits to society are enormous, but there are major risks for human rights associated with these technologies: automated face recognition brings privacy risks, targeted advertisement brings a risk of manipulation and undermining of democracy, and algorithmic discrimination threatens fairness [16].

In the area of cybersecurity, Big Data is being used a substitute for building secure systems: the focus shifts from prevention to ubiquitous monitoring, in which every person and object is monitored all the time with as goal to identify deviating behavior, which is acting as an indication of malicious behavior. In view of the scale of systems, this analysis needs to be automated with Artificial Intelligence (AI) techniques; the next step is predictive analytics, in which one tries to predict malicious behavior before it occurs. This approach is already being used by police forces, but may become more prevalent as technology progresses.

These developments impact human rights such as individual freedom and autonomy; moreover, the automation of security decisions with AI opens risks, as these decisions are not perfect. We have already mentioned algorithmic fairness/discrimination, based on incorrect data and biases. There is also the challenge of adversarial machine learning: it has been shown that deep learning algorithms can be fooled by making small changes to input [21, 20]. Finally, attackers will also resort to AI to evade the AI-based defense systems; this leads to a dystopian scenario in which AI-driven machines are combatting each other for control of the digital infrastructure. While it is unclear who will win, there is no doubt that privacy will be the first victim.

The emergence of **edge computing** [19] is driven by performance constraints; in view of the explosion of internet devices, there will not be enough bandwidth to send the data of all IoT devices to a central cloud infrastructure and not enough computing power to process all this data. Moreover, applications such as autonomous driving and robots require real-time responses, imposing the need for distributed intelligence, which is known as edge computing. This shift of intelligence towards the edge of the network enables privacy-friendly solutions as a by-product. However, if the edge model would be used to process data at the edge and collect intelligence in the cloud, it risks to making the surveillance infrastructure even more powerful.

2 Technology Risks: Data Breaches and Mass Surveillance

Humanity seems to have a problem with evaluating and managing big risks; one can think of climate change, nuclear risks (Chernobyl and Fukushima), risks related to the oil industry (Exxon Valdez and Deep Water Horizon), or financial risks (Lehman Brothers). Digital technologies and Big Data in particular seem to also belong in this category. We seem to be unable to prevent data breaches, and Big Data presents ever-bigger data breach risks, as visualized in [3]. Over the last years, billions of personal data sets have been leaked; several individual leaks have involved data related to hundreds of millions of personal data items. This includes very sensitive information such as information collected by dating websites (Ashley Madison), health websites (Anthem), credit risk companies (Equifax), social media (Facebook, Twitter) but also government databases. The most striking example is the breach of the US OPM (Office of Personnel Management) database – this database contains highly sensitive information of US government employees with a security clearance. This last case shows that these leaks are not only a privacy concern: they also represent a major security risk.

Privacy risks are typically perceived as individual risks: the privacy discussion is framed as the decisions of individuals whether to hide, control or exchange their information. This is based on the misunderstanding that personal data only affects a single person; however, by sharing personal data, we enable data analytics on personal data, which allows in turn identifying individual groups. The misuse of Big Data can lead to the outing of subgroups (e.g., of people with different sexual orientation or religious views), discrimination and even persecution. The tradeoff or dichotomy between collective security and individual privacy is a false one: privacy is also a collective good essential for protecting the values of our societies.

More in general, Big Data leads to large scale optimization, with as risk that the optimization targets are not aligned with the interests of the users or of society [17]. As an example, Waze may send large volumes of traffic to an 'optimal' route that happens to be close to a school. The same analogy holds: optimizing with Big Data may increase income of a single company or bring optimization to individuals but does not necessarily lead to results that are desirable for society as a whole.

The Snowden documents have increased global awareness and understanding of the extent to which governments have used the development of the digital society to deploy mass surveillance systems [14, 18]. Larger nations (and the smaller nations that collaborate with them) can analyze the contents of all our communications and stored data. Even if more encryption is used to protect this data, enormous amounts of meta data are becoming available, that show which services and devices we use, who we interact with, what we buy and where we are. While the term meta data sounds innocuous, meta data is data and there is no doubt that it allows to obtain highly sensitive information about a person including political preferences, social status, health status, and religion.

The Snowden revelations also show that government have methods access information held by industry (the NSA program for this access is aptly named

PRISM). In this context, the most relevant players are the large platforms that collect massive amounts of data on every interaction; most of them monetize this information through advertising ("data is the new oil); the term surveillance capitalism [13] has been coined to describe this business model. The justification for this mass surveillance by companies is that this data is used for specific purposes to which the user has agreed, that is, to learn aggregate information that benefits all or to improve the services for a specific user; intelligence services claim that they will only search for and identify bad guys, which corresponds to targeted surveillance. Human right activists will point out that in order to target individuals, massive amounts of data about everyone is being collected and stored, with a chilling effect on individual freedom ("we all know we are watched all the time) and with a strong potential for abuse or misuse, for example to target minority groups.

3 Crypto Wars: From Key Escrow to Cyber Weapons

Until the late 1980s, cryptography was expensive: cryptography was exclusively implemented in hardware devices that were tightly controlled. The use of cryptography was restricted to governments and the financial sector. Around 1990 the cost of cryptography started dropping and cryptography moved from hardware to software; the emergence of the World Wide Web created the need for secure transactions in open systems and made it much easier to distribute cryptographic software and know-how. While the increasing availability of cryptography for end-to-end encryption started to affect both intelligence services and law enforcement, the political debate at the time focused on the need for law enforcement to intercept communications. This gave rise to the (first) "crypto war." In 1994, the US proposed the Clipper chip for end-to-end encryption of telecommunications with built-in key escrow. The Clipper chip was quickly dropped due to technical shortcomings and protests from civil right groups, academia and industry. By the end of the 1990s, most export controls had been loosened and cryptography quickly became available in billions of devices. The 2013 Snowden revelations resulted in a further boost in the uptake of cryptography. Today one the number of cryptographic devices is larger than 30 billion; however, more than half these devices have as main goal entity or data authentication and protecting assets against users; only a fraction of the remaining ones offer robust end-to-end encryption of user data.

While this abundance of cryptography gave civil society the illusion that it won the crypto war, both law enforcement and intelligence services found many ways to get access to data: communications on mobile phones (2G-3G-4G) are not end-to-end encrypted, cryptographic standards were delayed and undermined [11], implementations were weakened (for example by introducing spoofed certificates), and legal tools were deployed to ask for cryptographic keys. In 2010 the open discussion resurfaced: law enforcement claimed that they were "going dark and demanded backdoor access to keys or data; this started a new battle in the crypto wars, this time dealing with access to many types of com-

municated and stored data; the risks related to such access are argued clearly by Abelson et al. [9]. While most players agree that weakening or backdooring cryptography presents a clear danger to the digital society, the debate goes on [7, 15]. At this stage, several countries (including Australia, Russia, and the UK) have enacted legislation that give governments the power to ask providers to backdoors to their equipment.

One cannot help but wonder whether the crypto war, and in particular the focus on escrowing of keys and/or weakening cryptography, is a diversion tactic. The spread of mobile devices and the expected growth of the IoT create huge amounts of meta data that are accessible to both law enforcement and intelligence services. Even if communications and stored data are encrypted, the location of devices and users, the communication patterns and the interests are collected and stored as Big Data; advanced analytics can be applied to this data, resulting in more information than ever before. Moreover, powerful attack tools (cyber weapons) are applied towards specific targets: by taking control of the end devices of the users, one can get real-time access to all the data, irrespective of the use of encryption for communicated or stored data; or one can undermine critical infrastructure. These cyber weapons are used by organized crime, companies that specialize in surveillance, law enforcement agencies, intelligence agencies and the military. In the latter case, they form part of offensive cyber warfare; several nations have publicly announced that they are making substantial investments in this area.

The development of sophisticated cyber weapons creates major risks for the digital society. First, these weapons are based on exploits of new unpatched vulnerabilities (so-called 0-days) in widely used software or hardware; the actors who develop these tools have an incentive to keep these vulnerabilities secret, rather than releasing them to the vendors under a responsible disclosure program or bounty process so that the vendors can fix the vulnerabilities. Hence, this approach undermines the security of the overall digital ecosystem, while our society becomes critically dependent on it. Second, controlling cyber weapons is difficult: once a tool is deployed and ends up in the hand of an adversary, he can reverse engineer it and repurpose it against other targets. Sometimes these tools are even leaked from the systems of the organization that created them (e.g., the hack of the company Hacking Team [8]). The collateral damage of the leakage of such tools can run in the billions of dollars. Third, for law enforcement applications these tools are problematic: once one has full control over the system of a target, one can easily frame the target. Fourth, attribution of cyber attacks can be very difficult, which increase the risks of incorrect responses and escalation. Today a growing number of nations is deploying such cyber weapons. While the convention of Geneva protects civilians in times of war, today cyber wars are being fought on civilian infrastructures in times of peace. It does not seem realistic to expect that the organizations who have acquired such cyber weapons will ever abandon them.

4 The Way Forward

The main concern created by the developments listed above is the concentration of power: the combination of mass surveillance by industry and governments with sophisticated cyber weapons creates an unprecedented situation: there is a risk that this power will be abused both in domestic and international policy. For industry, there is a growing risk that it will be drawn into this battle by providing information or by forced insertion of backdoors or logic bombs. In view of the complexity of the international supply chains, this will create strong tensions. Big Data can also be misused to violate human rights and to create unfair advantages for individuals or specific companies while damaging society. Citizens are on the losing end in this battle: while one would expect in a modern society that the powerful entities are transparent, while normal citizens have the right to privacy, technology developments have reversed this role: citizens are becoming fully transparent through technology, while the way governments and industry operates become increasingly opaque. Overall, this increase in power can only be mitigated by very strong democratic oversight mechanisms at national and international level supported by international agreements. A first step has been made by the Paris call for trust and security in cyber space [5].

In addition to a stronger governance, technical approaches can also help, but there are no silver bullets. Making progress will require strong collaboration between technologists and non-technical experts. Central elements are to build systems with privacy, security and transparency by design and to reflect societal values in all technology decisions. An important part of the solution is a radical choice for open solutions: open hardware and open software are the only way to create independence and to avoid backdoors. This should start with the building blocks (processors, e.g., Risk-V [6] and operating systems, e.g., Linux [4]) and the infrastructure (e.g., routers) but end with all applications. It is of course not sufficient to make all the details of hardware and software public: one needs powerful verification tools and governance mechanisms to support testing and verification. Creative thinking will be needed to develop new business models for an open world. A second part of the solution is decentralization: how to define decentralization is a topic by itself, but the current centralization of power is supported by the architecture of technologies. Technically it is possible to build more decentralized architectures that lead to decentralization of power ("architecture is politics, Mitch Kapor). A third element is the deployment of cryptographic techniques to protect data as it is stored, transmitted and processed; to the latter category belong techniques such as somewhat fully homomorphic encryption, secure Multi-Party Computation, and Functional Encryption; this approach allows to create value from the data while still protecting the data. More effort is needed to protect meta data.

Overall, one may have the impression that the way that digitalization has led to a centralization of power is inevitable. Hence, it may seem naïve to believe that it is possible to turn back the clock on some of these developments. There are indeed many hurdles to be taken, but the digitalization has also empowered individuals, has made it possible for ideas to spread and has enabled collabora-

tion at a global scale. In the end, humans will create the digital society and they are also capable of shaping this society in a way that it protects their rights and values.

References

1. California Senate Bill SB-327: Information Privacy: Connected Devices, 28 September 2018, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
2. EU Cyber Security Act, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
3. Information is Beautiful, Worlds Biggest Data Breaches and Hacks, http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks
4. The Linux Foundation, https://www.linuxfoundation.org/
5. Paris Call for Trust and Security in Cyber Space, https://pariscall.international/en/
6. Risk-V Foundation, https://riscv.org/
7. US National Academies, Decrypting the Encryption Debate. (2018) https://www.nap.edu/read/25010/
8. Wikipedia, Hacking Team, https://en.wikipedia.org/wiki/Hacking_Team
9. Abelson, H., Anderson, R.J. , Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B., Specter, M.A., Weitzner, D.J.: Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications. Communications of the ACM **58(10)**, 24-26 (2015)
10. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: A Survey. Computer Networks **54(15)**, 2787-2805 (2010)
11. Checkoway, S., Niederhagen, R., Adam Everspaugh, A., Green, M., Lange, T., Ristenpart, T., Bernstein, D.J., Maskiewicz, J., Shacham, H., Fredrikson, M.: On the Practical Exploitability of Dual EC in TLS Implementations. In: USENIX Security Symposium, pp. 319-335. Usenix (2014)
12. Chen, M., Mao, S., Liu, Y.: Big Data: A Survey. MONET **19(2)**, 171-209 (2014)
13. Foster, H.B., McChesney, R.W.: Surveillance Capitalism. Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. Monthly Review **66(3)** (2014)
14. Greenwald, G.: No Place to Hide, Edward Snowden, the NSA, and the U.S. Surveillance State. Metropolitan Books (2014)
15. Landau, S.: Listening In: Cybersecurity in an Insecure Age. Yale University Press (2017)
16. O'Neil, C.: Weapons of Math Destruction. Crown Books (2016)
17. Overdorf, R., Kulynych, B., Balsa, E., Troncoso, C., Gürses, S.: POTs: Protective Optimization Technologies. arXiv:1806.02711 (2018), https://arxiv.org/abs/1806.02711
18. Preneel B., Rogaway, P., Ryan, M.D., Ryan, P.Y.A.: Privacy and Security in an Age of Surveillance (Dagstuhl Perspectives Workshop 14401). Dagstuhl Manifestos **5(1)**, 25-37 (2015)
19. Satyanarayanan, M. The Emergence of Edge Computing. IEEE Computer **50(1)**, 30-39 (2017)

20. Shamir, A., Safran, I., Ronen, E., Dunkelman, O.: A Simple Explanation for the Existence of Adversarial Examples with Small Hamming Distance. arXiv:1901.10861 (2019), https://arxiv.org/abs/1901.10861
21. Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I., Fergus, R.: Intriguing Properties of Neural Networks. arXiv:1312.6199 (2013), https://arxiv.org/abs/1312.6199