CANVAS

Constructing an Alliance for Value-driven Cybersecurity

POLICY BRIEF NO. 2

CYBERSECURITY AND THE EUROPEAN DATA PROTECTION FRAMEWORK

The challenge: Several areas of conflict between data protection and security

Cybersecurity incidents can cover a very wide spectrum, including, e.g., hacking, blackmail encryption, and data or identity theft. There are diverse actors who could cause incidents affecting cybersecurity for different reasons. Moreover, such events can have varying, often unforeseeable impact, which can seriously undermine the availability, integrity, and confidentiality of digital technologies. This can involve the loss, compromise, or unauthorized disclosure of the personal data of individuals.

To achieve a better protection of individual’s fundamental rights with regard to the protection of their personal data, the European Union has adopted the General Data Protection Regulation (GDPR) mainly for the private sector, and Directive 2016/680 for the police and the justice sectors.

For Citizens, one of the biggest risks associated with cybersecurity is a violation of their privacy and the loss of data control.

The legislative process for a regulation on privacy and data protection to be applicable for electronic communications is still on-going. Nonetheless, these are the legal instruments to consider when determining conflicts as well as synergies to current cybersecurity legislation and policy arise.

The security vs. data protection trade-off view is a problem

It is known that measures aimed at enhancing cybersecurity may interfere with individual’s fundamental rights, especially their right to privacy and the protection of their personal data. For instance, consider a private actor (e.g., a company) refusing to grant data subject’s rights like the right to transparent information and access in order to protect his own business secrets. However, a much more prominent example subject to a public debate is the deployment of surveillance-oriented security technologies by state entities. In particular, national law enforcement and intelligence agencies. Many states, also within the EU, allow to varying degrees and with different preconditions, the deployment of such technologies, for instance Deep Packet Inspection, key

Lack of cybersecurity affects everyone

An example for a typical cybersecurity incident affecting a broad range of the world population is the so-called Mirai botnet. This malware was created and distributed in 2016 by students in the US who originally wanted to gain advantages in the online game Minecraft by launching a large-scale distributed denial of service (DDoS) attack. However, the botnet got out of control and infected a large number of IoT devices worldwide, such as IP cameras and home routers. This attack and the distribution of the malware was possible because Mirai exploited the fact that users rarely change the manufacturer's default usernames and passwords on their IoT devices. Once infected, an IoT device would become part of the botnet, being remotely controlled for large-scale network attacks. In October 2016, the attack got to a point where it almost completely brought down the internet in the entire eastern United States. The device owners themselves seldom noticed the malware infection because the devices continued to function normally, except for some lag in response times and increased usage of internet bandwidth.

escrow, back-doored encryption tools, and stockpiling security vulnerabilities (so-called zero-day exploits). Yet, the use of technology to infiltrate citizens' devices and communications in order to find criminals has been repeatedly criticized as coming along with significant risks of misuse, bias, and lack of transparency. There is a common belief among government officials in the field of police and national security that the combat of crime justifies the means, namely sacrificing the general security of technical devices for everyone by deploying surveillance-oriented technologies. However, many security researchers warn of unintended side-effects and consequences like unauthorized use of surveillance tools, or unresolvable discrepancies when governments don't decide clearly for either offensive or defensive strategies. Furthermore, there is the matter of so-called function creep, which means the extension of deployment purposes that can cause violation of democratic principles and values.

Is weakening security the right way to achieve security?

In 2011, the German Chaos Computer Club (CCC) discovered a Trojan Horse malware ('Bundestrojaner', translated: 'Federal Trojan' or 'State Trojan') that surveilled targeted devices, thereby enabling backdoor remote control. The revelation of the use of this malware triggered criticism for weakening the security of the targeted device. It was argued that not only law enforcement, but also criminals and authoritarian states could make use of such functionalities. The revelation sparked a large public debate around the legality of using such technologies in democratic societies.

In this context, the proportionality principle is a hugely difficult issue, besides the general question whether broad surveillance of a large part of the citizenship should be allowed in a democratic society. Such large-scale intrusiveness of state surveillance for security purposes can pose the danger of an erosion of privacy and other fundamental rights and democratic principles. Examples are the presumption of innocence and the prohibition of penalties without law, for example by assigning a higher crime risk to individuals on the basis of assumptions, and thus making them a focus or target of police activity, or a person being placed under suspicion because of few, uncertain or selectively chosen circumstantial, personal or behavioral factors. Thus, it all comes back to the need of transparency and effective checks and balances aligned to the principle of proportionality, while these are also key principles in European data protection law.

In the private sector, economy trumps security and data protection alike

Cybersecurity and data protection are also relevant for the private actors. Not only because the aforementioned governmental entities increasingly rely on private actors as information sources, but also because of economic reasons. In the business sphere, there are often processes for the management of IT security. However, these internal departments and team members are often also tasked with data protection matters despite the fact that IT security and data protection have very different viewpoints, goals, and expertise requirements. Regardless of the internal organization, personal data protection can be a complex and context-dependent matter, while often reducing the entity's possibilities to pursue its own economic interests, which especially applies to data-driven businesses.

Technical and organizational measures both of IT security and data protection can be costly and difficult to deploy. This affects the whole private sector, including those fields where data controllers are handling sensitive personal information, such as health data, and could be even classified as part of a critical infrastructure. For example, many medical offices, hospitals, and medical research institutions lack the funding to comprehensively employ IT security measures needed. Moreover, they often also lack the expertise to do so.

EU citizens want it all – security, privacy and data protection

Various studies and research activities across the EU have found that European citizens wish for a more comprehensive approach to security and data protection. In the health sphere, citizens appear to be especially sensitive to the handling of their health data. Consent and trust for the recording, processing, and storing of such data depend on the context. In the business sphere, citizens are also concerned with privacy infringements. There is a lack of trust in private businesses regarding the use of personal data, as well as a concern with internet and e-commerce security. In the police and national security sphere, there is diversity in the perception of the role of the state and of value-sensitive technologies. Citizens find national security measures more acceptable if they view the state as a guardian rather than an intruder, which depends on their experience and their country's history.

Overview of issues related to cybersecurity

- Lawful access‘ exploits can be loopholes for malicious parties
- Difficult actor allocation for cybersecurity incidents
- Increasing dependence on vulnerable IT
- Rapidly developing technology
- Risk of misusev
- Legal and factual frame conditions often unclear
- Offensive measures can weaken security for everyone
- Citizens do not want a privacy vs security trade-off
- Many cybersecurity measures rely on surveillance
- Commplex playing field of actors, lack of transparency
- Varying and unforeseeable impact of incidents
- Data driven businesses do not want to invest in security and data protection
- Infringement on privacy as constitutional right
- Intrusiveness of security tools challenging privacy
- Cybersecurity is a very complex global issue.
- ‘Arms race‘ of offensive strategies

Responsibilities of the data controllers are key

From a data protection point of view, the responsibilities of the data controllers are most relevant in the context of cybersecurity. According to the GDPR, data controllers and processors have a legal obligation to implement appropriate technical and organizational measures to protect the personal information they intend to collect and process. In some cases, a Data Protection Impact Assessment has to be conducted first. The measures that need to be deployed depend on case, situation, and state of the art in specific areas. This is the point where synergies with cybersecurity measures become possible because even though there are cybersecurity measures which may conflict with the safeguarding of data subject's rights, there are also measures that enhance data protection. Examples of such preventive or reactive measures are access control, encryption, data separation, anonymization, pseudonymization, records of processing activities, technical and organizational procedures for backup and restore, logging, and pre-defined data breach notification procedures. In the context of technical and organizational measures, both the GDPR and Directive 2016/680 manifest specified requirements to ensure the security of processing with respect to confidentiality, integrity, availability, and resilience of IT systems and services in the context of personal data processing.

Such measures can also be part of a data protection by design and by default approach. With the new legal framework, non-compliance is now more likely to lead to negative consequences for the controllers because they must demonstrate compliance, while competent data protection supervisory authorities now have increased enforcement powers. Therefore, it is advisable for data controllers to establish an effective data protection management procedure within their own organization. In addition, yearly security checks, audits, and the implementation of best practices from the security domain, such as penetration tests and keeping track of security incidents are reasonable measures to achieve and demonstrate compliance.

Solution possibilities summarized: Pursue and foster holistic approaches

At the moment, a lot of divisive factors exist across the European Union member states, which need to be overcome. By using possible synergies between security and data protection approaches and measures, much more (also cost-effective) positive impact on cybersecurity can be achieved. Security measures, technologies, and application scenarios should be carefully assessed before seeking public acceptance. Thereby, a more careful balance should be struck that is more aimed at unifying the objectives of security, privacy, data protection, and fundamental rights instead of following the classical trade-off view. In this context, technical and organizational measures of privacy, data protection, and (cyber) security can be mutually reinforcing. Therefore, those expert fields and domains can learn a lot from each other, which is why future, holistic and interdisciplinary research should be supported. Beyond these aspects, transparency, trust, and checks and balances are key issues to achieve value-based cybersecurity. It is advisable in a first step to consider these values for the nearer future in the legislation process for the regulation of privacy in electronic communications. Thereby, an emphasis should lie on the reinforcement of controller obligations to implement transparency, user control, and security measures, as well as enhanced accountability and enforcement mechanisms.

Where more info can be found

This Policy Brief is based on the research work done by the CANVAS project (Constructing an Alliance for Value-driven Cybersecurity). Detailed reports of this work have been published in four main White Papers:

1. Cybersecurity and Ethics
2. Cybersecurity and Law
3. Attitudes and Opinions Regarding Cybersecurity
4. Technological Challenges in Cybersecurity

All White Papers can be found on our website, along with all of our (downloadable and printable) Policy Briefs, short online explanations of the key cybersecurity issues, and commented literature lists for further reading:

canvas-project.eu

Co-funded by the Horizon 2020 programme of the European Union

The CANVAS project (Constructing an Alliance for Value-driven Cybersecurity) has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540. This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 16.0052-1. The opinions expressed and arguments employed therein do not necessarily reflect the official views of the Swiss Government.

Objective of CANVAS:
To bring together stakeholders from key areas of the European Digital Agenda to approach the challenge how cybersecurity can be aligned with European values and fundamental rights.

Partners:
The CANVAS Consortium consists of 11 partners (9 academic institutions and 2 partners outside academia) located in 7 European countries.

Version and date of publication:
Version 1.0, February 2019

Funding:
1.57 Mio. €, of which 1 Mio. € is funded by the European Commission and the remaining part emerges from the Swiss State Secretariat for Education, Research and Innovation.

Project coordination and contact:
PD Dr. sc. ETH Markus Christen, University of Zurich (UZH), Digital Society Initiative, Rämistrasse 66, 8001 Zürich

Project duration:
September 2016 – August 2019