POLICY BRIEF NO. 2

CYBERSECURITY AND THE EUROPEAN DATA PROTECTION FRAMEWORK

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

Often, cybersecurity incidents involve the loss, compromise, or unauthorized disclosure of the personal data of individuals.

Incidents can cover a very wide spectrum
including, e.g., hacking, blackmail encryption, and data or identity theft.

Many different actors
could cause cybersecurity incidents for various reasons.

Events can have varying, often unforeseeable impact,
which can seriously undermine the availability, integrity, and confidentiality of digital technologies.

Many challenges and conflicts for cybersecurity and data protection

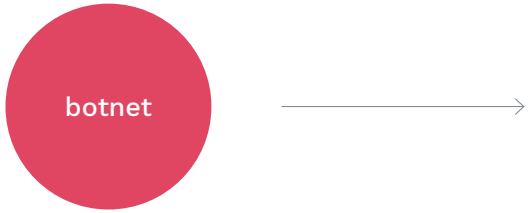
- Data-driven businesses do not want to invest in security and data protection
- Citizens do not want a privacy vs security trade-off
- Infringement on privacy as a constitutional right
- Risk of misuse
- Intrusiveness of security tools challenging privacy
- Rapidly developing technology
- Increasing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

- Lack of support for SMEs, e.g. by funding and training schemes for better IT security
- Still widespread lack of baseline security, becoming more urgent with the rise of IoT
- Lack of support for SMEs, e.g. by funding and training schemes for better IT security

Lack of cybersecurity affects almost everyone

An example for a typical cybersecurity incident which affected a broad range of the world population is the so-called Mirai botnet.

Originally, young students just wanted to cheat in an online game by creating the Mirai botnet to bring the game server down. But the botnet got out of control. Infected devices became part of the botnet, being remotely controlled for large-scale network attacks. In October 2016, the attack almost completely brought down the internet in the entire eastern United States.



Botnets consist of infected devices, such as computers and IoT (Internet of Things) devices, that are controlled by a malicious party. IoT is the term for connected electronic devices being able to exchange data, e.g. via the internet. Examples are internet routers, cameras, TV's, or digital video recorders.

The new European data protection framework matters

In Europe, the protection of citizen's personal data is regulated by the **General Data Protection Regulation (GDPR)**, and **Directive 2016/680** (for the police and the justice sectors).

Still ongoing is the legislation process for a regulation on privacy and data protection to be applicable for electronic communications (**ePrivacy Regulation**).

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

It is known that some measures aimed at enhancing cybersecurity can interfere with individual's fundamental rights, in particular with their right to privacy and the protection of their personal data.

Example 1

A private company wants protect its business secrets and thus deploys internal security measures, such as strict access control. But to this end, even valid data subject's rights like the right to transparent information and access, are denied.

Example 2

Law enforcement and intelligence agencies often rely on surveillance-oriented security technologies to do their work and occasionally demand more powers in that area. But many of those technologies, like Deep Packet Inspection, or stockpiling and using existing security vulnerabilities in software, can weaken security and privacy for everyone.

Surveillance-oriented security technologies can be dangerous

Does the combat of crime justify the means, i.e. sacrificing the security of technical devices in general and for everyone?

The use of technology to infiltrate citizen's 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.**

Security researchers have warned against **unintended side-effects** like surveillance tools falling into the hands of criminals, or malicious actors using the same software vulnerabilities than law enforcement does.

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.

Citizens do not want to be surveilled all the time

Should technology help in making people a focus or target of police activity by assigning a **higher crime risk to individuals on the basis of assumptions**?

What about transparency, boundaries, and effective checks and balances when a person is **constantly watched because of a few, uncertain, or even selectively chosen circumstantial, personal or behavioural factors**, such as being poor, living in the wrong district, or having a different skin colour?

Fairness, the rule of law, and due process

Large-scale intrusiveness of state surveillance can foster erosion of privacy and other fundamental rights and democratic principles.

Democratic principles like the presumption of innocence and the prohibition of penalties without law are at stake.

Proportionality 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.

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

Security and data protection can be obstacles for a company's economic interests, especially when it relies on data-driven business.

In the business sphere, many companies don't do enough in terms of cybersecurity and data protection due to the **attached costs** to set up and maintain effective IT security as well as data protection management processes.

To save money, internal IT security experts get very often tasked with data protection matters too. However, this is **counterproductive** since IT security and data protection usually have very **different viewpoints, goals, and expertise requirements**.

Lack of investment affects also critical infrastructures

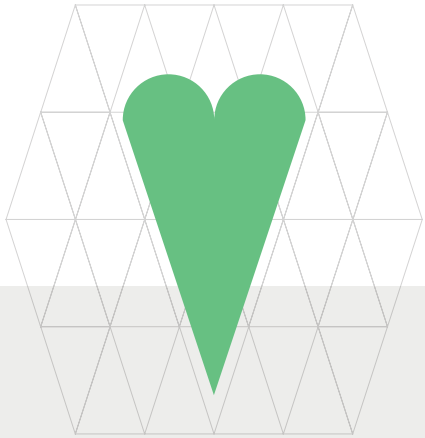
The costs to deploy technical and organizational measures are frequently deemed too high, even in areas where data controllers are handling sensitive personal information, such as health data.

Public health institutions are classified as part of a country's critical infrastructure.

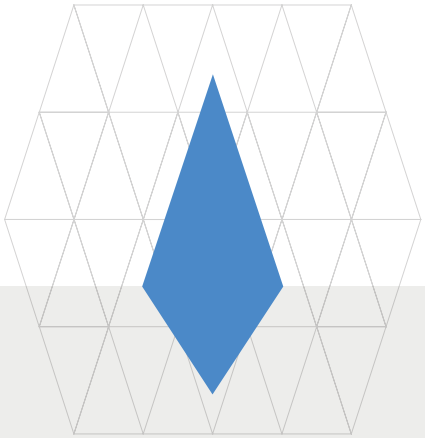
Still, many medical offices, hospitals, and medical research institutions **lack the funding and the expertise to comprehensively employ necessary measures** to prevent e.g. medical devices getting infected with viruses, or health data getting lost or compromised.

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

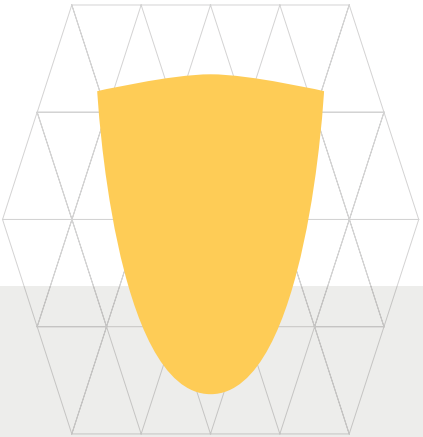
Various studies and research activities across the EU have found that European citizens wish for a more comprehensive approach to security and data protection.



In the **health sphere**, citizens appear to be especially sensitive to the handling of their health data. Consent and trust highly depend on who they share the data with and in which context.



In the **business sphere**, citizens also worry about privacy infringements and IT security, especially when using internet services like online shops. They do not have much confidence that private corporations handle their personal data in a responsible manner.



In the **police and national security sphere**, citizens deem national security measures more acceptable when they view the state as a guardian rather than an intruder, which often depends on experience and country history.

Responsibilities of the data controllers are key

According to the GDPR, data controllers and processors of personal data have a legal obligation to implement appropriate technical and organizational measures to protect this data. 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. Synergies between cybersecurity and data protection solution approaches exists and should be used.

Exemplary technical and organizational measures

- Access control
- Encryption
- Data separation
- Anonymization
- Peudonymization
- Records of processing activities
- Procedures for backup and restore
- Logging
- Pre-defined data breach notification procedures.

Both the GDPR as well as the Directive 2016/680 regulate specific security requirements for IT systems and services with respect to their

- confidentiality,
- integrity,
- availability,
- and resilience
- in the context of personal data processing.

Effective management procedures and Privacy by Design can help

Data controllers and processors must deploy reasonable measures to demonstrate compliance with the GDPR.

It is advisable for data controllers to **establish an effective data protection management** within their own organization that is **separate** from the IT security department, **but works closely with it**.

In addition, yearly **security checks, audits, and the implementation of best practices** such as from the security domain can enhance both cybersecurity and data protection. Examples are penetration tests and keeping track of security incidents.

Summarized: Apply value-driven and interdisciplinary approaches

- Recognize **transparency, trust, and checks and balances** as the key issues to achieve value-based cybersecurity.
- Consider these **values** in the legislation process for **the upcoming ePrivacy regulation** for electronic communications.
- Security measures, technologies, as well as application scenarios should be subjected to a **data protection impact assessment**.
- **Discard** the security vs privacy trade-off view.
- Rather, aim for a more **careful balance** with fair and lawful compromises between security, privacy, data protection, and fundamental rights.
- **Use synergies** between cybersecurity and data protection approaches and measures.
- **Reinforce** controller and processor obligations and accountability.
- **Support** interdisciplinary research.

More information can be found

The slides are based on the research work done by the CANVAS project (Constructing an Alliance for Value-driven Cybersecurity).

The objective of CANVAS is 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.

In particular, we provide the following CANVAS resources:

- Briefing packages
- CANVAS Reference Curriculum
- CANVAS MOOC
- Open Access Book
  'The Ethics of Cybersecurity'

The following slide directly points to those of our White Papers which address in detail the challenges of cybersecurity.

Bibliography: cybersecurity challenges (CANVAS White Papers)

Ethical challenges

Yaghmaei, Emad, Ibo van de Poel, Markus Christen, Bert Gordijn, Nadine Kleine, Michele Loi, Gwenyth Morgan, and Karsten Weber. 2017. “Canvas White Paper 1 – Cybersecurity and Ethics.” SSRN Scholarly Paper ID 3091909. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091909.

Legal challenges

Jasmontaite, Lina, Gloria González Fuster, Serge Gutwirth, Florent Wenger, David-Olivier Jaquet-Chiffelle, and Eva Schlehahn. 2017. “Canvas White Paper 2 – Cybersecurity and Law.” SSRN Scholarly Paper ID 3091939. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091939.

Technological challenges

Domingo-Ferrer, Josep, Alberto Blanco, Javier Parra Arnau, Dominik Herrmann, Alexey Kirichenko, Sean Sullivan, Andrew Patel, Endre Bangerter, and Reto Inversini. 2017. “Canvas White Paper 4 – Technological Challenges in Cybersecurity.” SSRN Scholarly Paper ID 3091942. Rochester, NY: Social Science Research Network.

https://papers.ssrn.com/abstract=3091942.

Project facts

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

Slidedocs version:
Version 2.0 October 2019

Project duration:
Sept. 2016 – Oct. 2019

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

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.

Funding notice for CANVAS

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 EU and the Swiss Government