INAUGURAL LECTURE

Mortaza Shoae Bargh

Realizing Secure and Privacy-Protecting Information Systems:

Bridging the Gaps

Realizing Secure and Privacy-Protecting Information Systems:

Bridging the Gaps

Hogeschool Rotterdam Uitgeverij

Colophon

ISBN: 9789493012080
1st edition, 2019

This book is a publication by Hogeschool Rotterdam Uitgeverij
P.O. box 25035
3001 HA Rotterdam

Publication can be ordered by contacting
www.hr.nl/onderzoek/publicaties

Realizing Secure and Privacy-Protecting Information Systems:

Bridging the Gaps

Mortaza Shoae Bargh

Research Professor Privacy & Cybersecurity

June 27, 2019

Abbreviations

AI	Artificial Intelligence
APT	Advanced Persistent Threat
ARPA	Advanced Research Project Agency
ASP	Application Service Provider
BYOD	Bring Your Own Device
CAGR	Compound Annual Growth Rate
CIA	Confidentiality, Integrity and Availability
CNSS	Committee on National Security Systems
DDoS	Distributed Denial of Service
DECODE	DEcentralised Citizen-owned Data Ecosystems
DNS	Domain Name System
DoS	Denial of Service
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EU	European Union
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IoT	Internet of Things
IS	Information System
ISP	Internet Service Provider
OECD	Organization for Economic Co-operation and Development
PC	Personal Computer
PET	Privacy Enhancing Technology
RCP&C	Research Chair on Privacy & Cybersecurity
RUAS	Rotterdam University of Applied Sciences
SDLC	System Development Life Cycle
SecSDLC	Security Systems Development Life Cycle
SME	Small and Medium-sized Enterprise
SOC	Security Operations Center
TADR	Transitional Action Design Research
TTP	Trusted Third Party
UAS	University of Applied Sciences
UASs	Universities of Applied Sciences
US	United State
USD	United State Dollar

Foreword

Continuous development and increasing usage of Information and Communication Technologies (ICT) introduce many opportunities for individuals, organizations and the society at large. For example, people can get in touch with their friends and families, get entertained via digital media, and use e-services in the comfort of their homes. The usage of ICT, however, increases also people's dependency on the well-functioning of Information Systems (ISs), which are, in turn, based on ICT. This dependency on ISs introduces increasing risks for individuals, organizations and the society.

Privacy and cybersecurity risks constitute two important categories of such IS risks. Privacy risks exist because a large amount of personal data is produced by and collected via ISs. For example, smart phones and sensors collect data about people and their immediate and private environments. Further, public organizations and commercial companies register and collect information about individuals directly for administrative purposes or for offering their services. This proliferation of personal data via ISs makes people vulnerable to privacy risks. In addition to privacy risks, ISs are subject to various cybersecurity risks, like hacking and denial of service attacks. These cybersecurity risks can potentially bring the society to a standstill as most of the social, economic, administrative and government services rely on the well-functioning of ISs. Privacy and cybersecurity risks can inflict adverse impacts on the lives, liberties, autonomy, dignity and property of individuals as well as on the interests of organizations, companies and the society at large. These risks can be caused intentionally by illegitimate intruders as well as unintentionally by legitimate but oblivious personnel.

In order to address and contain privacy and cybersecurity risks, there is an increasing need for protecting ISs and the personal data that are collected by, stored in, and analyzed within these systems. This need shapes the mission of this research chair. The field of privacy protection and cybersecurity has a wide scope, which can be approached from different directions, for example, individual (scientific) disciplines, system operation process, and system development process. The Research Chair on Privacy & Cybersecurity at Rotterdam University of Applied Sciences will focus on and adopt the last direction, namely the system development viewpoint. The mission of this research chair can be formulated as: How to realize privacy-protecting and secure ISs in practice? Currently, there are gaps between the existing approaches and what is needed in practice. Bridging

these gaps requires further research as well as embodiment of the research results in education curricula.

The field of privacy protection and cybersecurity, in general, and the realization of privacy-protecting and secure ISs, in specific, have often been characterized as a combination of art and science (Whitman & Mattord, 2011). Privacy protection and cybersecurity are art, as there are no concrete rules to regulate selection and configuration of various data protection and security mechanisms. Privacy protection and cybersecurity are science, as there are many sound and approved methods, techniques and guidelines to realize privacy-protecting and secure ISs. Privacy protection and cybersecurity, further, are closely related to humanities and social science, as ISs are used by people within organization, intentionally or otherwise. These users are considered as the weakest link in the chain of the measures devised and used for protecting privacy and securing ISs. Therefore, system designers, implementers and administrators should understand users' behavior in their societal and organizational context.

As a starting point, this contribution elaborates on a number of the existing gaps and discusses some possible directions for bridging these gaps. In particular, for realizing privacy-protecting and secure ISs, one needs to bridge the gap between non-technological – e.g., ethical, legal, social and economic – aspects and technological ones. Bridging these gaps is at the center of the focus of this research chair. This bridging leads to devising socio-technological solutions for privacy and cybersecurity risks. Such solutions rely on both technological and non-technological measures. This contribution describes also the often-overlooked interplay between privacy protection and cybersecurity in protecting distributed ISs such as the Internet of Things (IoT). This interplay asks for, among others, adopting an integrated approach for protecting such systems.

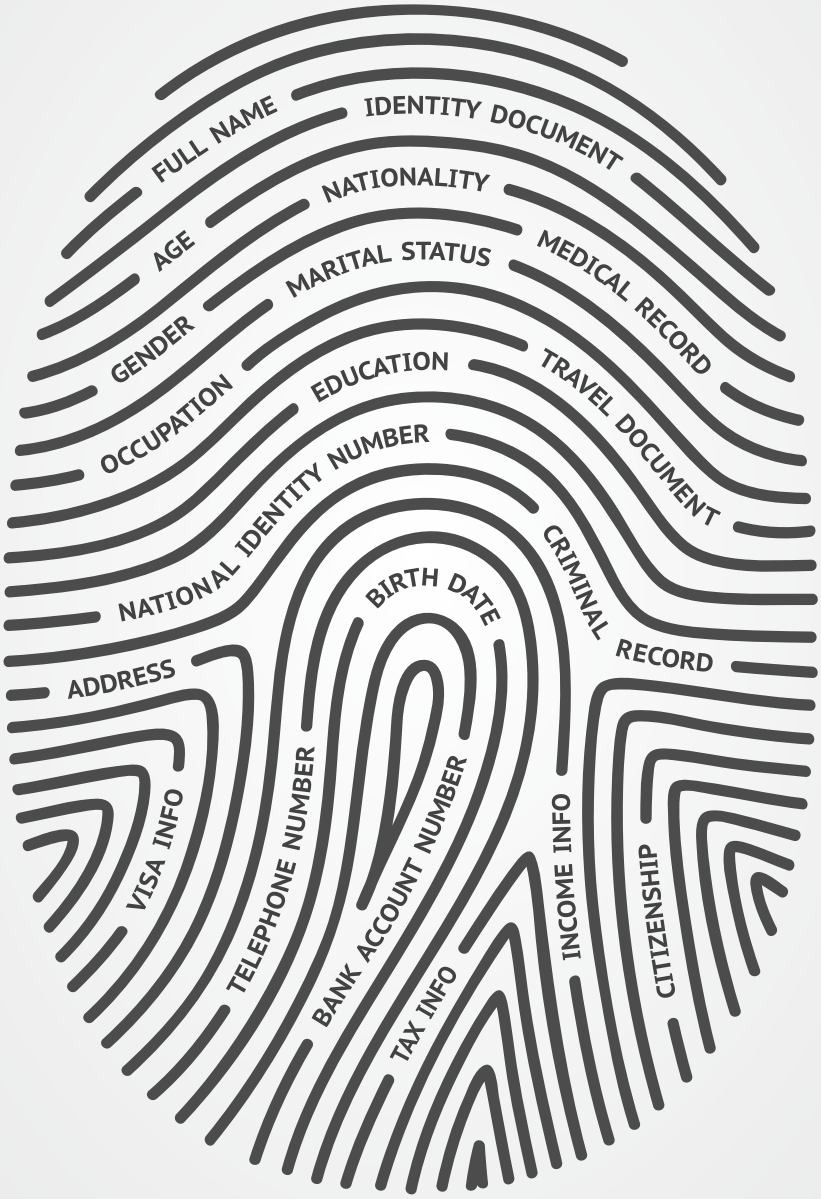
As a research direction, the contribution suggests developing and adopting an IS design methodology based on the design-thinking and engineering approaches. Such a methodology can enable the realization of privacy and security by design principles in a systematic way. As another research direction, the research chair is going to study technological measures at various levels (e.g., architectural, protocol and algorithmic levels) to automate parts of the data protection and security processes and develop (ICT) tools to support field experts and end-users in protecting ISs and the personal data therein. These technological measures can be devised for various stages of data analytics processes and artificial-intelligence-based systems, such as data collection, model extraction, and model-outcome interpretation. These technological measures are complimentary to non-technological measures so that data can be collected, processed and used in a fair and responsible way as foreseen in, for example, ethics as well as privacy laws and regulations.

This contribution is based on, among others, a number of the author's publications in recent years. Many coauthors have contributed to these publications that I would like to extend my sincere gratitude to each of them, in particular: Sunil Choenni, Ronald Meijer, Niels Netten, Susan van den Braak, Marco Vink and Maaike Harbers. Collaboration with my coauthors has been instrumental to shape the thoughts presented in this contribution. My sincere appreciations go to my colleagues at the Research Center Creating 010, Rotterdam University of Applied Sciences, as well as my colleagues at the Research and Documentation Center, Ministry of Justice and Security, for creating a warm environment for collaboration and research. Further, I am grateful to the executive board of Rotterdam University of Applied Sciences, Paul Rutten (the director of the Research Center Creating 010) and Sunil Choenni (the head of Statistical Data and Policy Analysis Division of the Research and Documentation Center) for placing their trust and confidence in my abilities to assume the Research Chair on Privacy & Cybersecurity.

This journey was impossible without unconditional love and support of my family. Dear Kimia and Armin, thank you for understanding your father's job and hobby as researcher, as it often extends beyond official working hours. Dear Behnaz, your love, support and affection made it possible for me to come so far. I am eternally grateful for having you beside me!

June 3, 2019
Mortaza S. Bargh

Table of contents


FULL NAME
IDENTITY DOCUMENT
NATIONALITY
AGE
MARITAL STATUS
MEDICAL RECORD
GENDER
EDUCATION
TRAVEL DOCUMENT
OCCUPATION
NATIONAL IDENTITY NUMBER
CRIMINAL RECORD
BIRTH DATE
ADDRESS
VISA INFO
TELEPHONE NUMBER
BANK ACCOUNT NUMBER
INCOME INFO
CITIZENSHIP
TAX INFO

Safeguarding the (impacts of) digital world

Information and Communication Technologies (ICT) – comprising hardware components (like sensors, smart devices, computers and communication networks) and software components (like games, mobile apps, desktop applications and digital services) – have created a ubiquitous digital world around us. This digital world provides new capabilities and opportunities for individuals and businesses to interconnect, access information, carry out intelligent analysis and execute (a new range of) activities in a fast and easy way. In addition to offering many opportunities, ICT inflict many risks upon individuals, organizations and the society. Privacy and cybersecurity risks are two important categories of such risks. Addressing privacy and cybersecurity risks is the focus of the Research Chair[1] on Privacy & Cybersecurity (RCP&C) at Rotterdam University of Applied Sciences (RUAS). As the starting point, this contribution aims at depicting the landscape of privacy and cybersecurity as well as describing the (research) activities of the RCP&C in the coming years.

To set up the context and the scope of the RCP&C, this chapter starts with highlighting the importance of safeguarding the digital world (Section 1.1) and motivates the growth of privacy protection and cybersecurity based on its market share (Section 1.2), the driving forces behind the market share (Section 1.3), and the perspectives of its job market (Section 1.4). Subsequently, the approach of the RCP&C is going to be described in Section 1.5. Finally, the scope and outline of the rest of the contribution are given in Section 1.6.

1.1 Importance of safeguarding

Nowadays almost every aspect of people's lives, individually or collectively (e.g., within a community, a company, an organization or the society), is dependent on the well-functioning of the digital world. This dependency is ubiquitous, spanning private, public and business spheres. The digital world serves many purposes, for example, for provisioning vital services like those in healthcare and for

1 Throughout this contribution the term 'research chair' is adopted for both 'lectoraat' and 'lector' in Dutch.

provisioning e-government services like filing tax returns. Last but not least, the ICT create new business opportunities and products, like those provided by Google, WhatsApp, Instagram, Amazon, bol.com and Spotify.

Unfortunately, there is no guarantee for the well-functioning of the digital world all the time due to, among others, its complexity and its potential for misuse. Firstly, the complexity of ICT and the interdependencies between technologies, organizations and people within the digital world create many vulnerabilities for malfunctioning, faults and intrusions. Such faulty operations and malfunctioning can bring many vital services that daily life depends on to a standstill situation or may even inflict severe safety hazards and risks upon people. Secondly, all the (new) capabilities and opportunities of the digital world are also available for criminals to carry out their illegal activities and for unethical opportunists to misuse ICT for their own personal benefits.

Not only do ICT serve as an accelerator for existing crime types, they also enable new crime types (Bargh et al., 2012). (Organized) cybercrime has become a rising concern of all nations in this golden ICT age. Cybercrime inflicts enormous costs on society, businesses and individuals. According to a study conducted by TNO[2], cybercrime costs The Netherlands more than 10 billion euros annually (de Ruiter, 2012). This is about 1.5 to 2% of the country's Gross Domestic Product (GDP), being comparable to the 2010 economic growth of the country. There is also some evidence that cybercrime costs increase steadily. Cybercrime causes also nonfinancial damages. Not only does it endanger the integrity and reputation of individuals, but also, at large, it hurts the customer's trust in e-services.

In recent years the field of privacy protection and cybersecurity have gained a key role for safeguarding the well-functioning of the digital world and the underlying ICT infrastructures and applications. This field deals with complex socio-technological systems (Mumford, 2006), involving various parties like end-users, ICT devices/machines, commercial companies and societal institutions. Therefore, the field is multi-disciplinary by definition. Although the breeding ground is technology mainly, a multi-disciplinary approach can deliver a privacy-protecting and secure digital world, as will be elaborated upon in the following chapters of this contribution.

---

2 TNO is in Dutch an abbreviation of the Netherlands Organization for Applied Scientific Research, webpage http://www.tno.nl/.

1.2 Market share for privacy protection and cybersecurity

The market share of the field of 'privacy protection and cybersecurity'[3] is experiencing a steady rise in the coming few years, as anticipated by some commercial market research agencies. For example, the Compound Annual Growth Rate (CAGR) of the privacy protection and cybersecurity field is expected to be

- About 10.2% during 2018-2023, expanding from USD 152.71 billion in 2018 to USD 248.26 billion by 2023, according to the report published by MarketsandMarkets[4],
- About 11.9% during 2018-2025, expanding from USD 104.60 billion in 2017 to USD 258.99 billion by 2025, according to the report published by Allied Market Research[5], and
- About 12.0% by 2024, expanding to more than USD 300 billion by 2024, according to the report published by Market Study Report[6].

Overall, the above figures indicate that the global industry outlook for privacy protection and cybersecurity is very positive and looks promising. According to (Pendse, 2018) from Nasdaq Global Information Services, "the actual spending on cybersecurity may be far more than what's revealed publicly, as companies may be understating their cybersecurity budgets in order to protect their reputations."

The market share of privacy protection and cybersecurity within the Netherlands shows similar trends of high growth. According to a survey conducted amongst ICT companies by SEO Amsterdam Economics – commissioned by the Dutch Ministry of Economic Affairs (Hendriks et al., 2016) – the size of the Dutch cybersecurity sector was about 10% of the whole turnover within the ICT sector in 2014, with an estimated sector's added value of 3.8 to 4.1 billion euros. This amounts to approximately 0.6% of the Dutch GDP in 2014. Hendriks et al. (2016) conclude that the cybersecurity sector grew 14.5%, faster than the ICT sector itself.

---

3 Note that the information sources cited in Sections 2.2, 2.3 and 2.4 present the figures and numbers under the generic term of cybersecurity. To comply with the terminology adopted throughout this contribution, the term 'privacy protection and cybersecurity' is used instead of the generic term cybersecurity in Sections 2.2, 2.3 and 2.4.

4 See Cybersecurity Market, https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html and Cybersecurity Market Worth $248.26 Billion by 2023, https://www.prnewswire.com/news-releases/cybersecurity-market-worth-248-26-billion-by-2023-893372986.html, Chicago, September 21, 2018.

5 See Global Opportunity Analysis And Industry Forecast, 2018-2025, https://www.alliedmarketresearch.com/cyber-security-market, March 2019.

6 See At 12% CAGR, Cybersecurity Market Size will reach 300 billion USD by 2024, https://www.marketwatch.com/press-release/at-12-cagr-cybersecurity-market-size-will-reach-300-billion-usd-by-2024-2019-02-13, February 13, 2019.

1.3 Driving forces behind the market growth

A number of driving forces are mentioned behind the market growth of privacy protection and cybersecurity. Examples are the emergence of disruptive ICT, the rising need for specific privacy and cybersecurity solutions, and the strategic plans of businesses not to become a victim of privacy and cybersecurity risks. In the following, some of these factors are listed, mainly from the sources cited in the previous chapter (i.e., the market research reports of MarketsandMarkets, Allied Market Research, and Market Study Report).

The emergence of disruptive ICT, such as the Internet of Things (IoT) and Bring Your Own Device (BYOD), and the increasing adoption of these technologies across industry segments and within organizations, have exposed people to various risks, specially the risks of Advanced Persistent Threats (APTs) that provide unauthorized access to an asset (like someone's computer) without being detected for an extended period. To save monetary or energy costs, IoT devices are often manufactured without basic security features. Therefore, such devices become attractive for cybercriminals and intruders to exploit the IoT's vulnerabilities for their own malicious purposes. In addition, it has become increasingly difficult for organizations to manage their devices and the growth of data flows via these systems. Consequently, the need for tools and systems that protect ICT systems and the information flows therein has increased.

Rising needs for specific cybersecurity solutions, such as strong authentication techniques, are going to boost privacy protection and cybersecurity market. Cloud computing has become attractive for organizations, especially for Small and Medium-sized Enterprises (SMEs), as it reduces the burden of having and managing ICT systems. Organizations, however, are potentially becoming more exposed to external risks (e.g., data breaches) when adopting cloud computing. To deal with these risks, organizations may adopt multi-factor authentication to mitigate the risks of password-based authentication. Multi-factor authentication adds another authentication step (e.g., sending a token via an SMS message) to the traditional authentication method of using a username and password.

Including privacy protection and cybersecurity activities as part of the strategic business plans has gained importance in commercial companies and enterprises. Minimizing the damage of ICT resources due to privacy and cybersecurity risks is currently prioritized highly in these companies. The objective is to prevent reputation damages and/or even foster the trustworthiness of these companies, thus gaining a cutting-edge business value out of being trustworthy.

Other driving factors mentioned are the increase in the frequency and sophistication of cyber threats caused by, for example, malware, ransomware and phishing messages, and the rising threat of global cyberterrorism. Stringent

regulations for privacy protection and cybersecurity, like the EU's new General Data Protection Regulation (GDPR) which came into force on the 25th of May 2018, are also perceived as another contributor to the rise of their market share.

1.4 Job market

Dearth of privacy protection and cybersecurity experts is considered a major impediment to deal with and meet the market demands. At the start of 2018, there were about half million cybersecurity job vacancies in the US alone. According to the Bureau of Labor Statistics of the US department of Labor, the rate of growth for jobs in information security is projected to be at 28% in the period of 2016–2026 (Occupational Outlook Handbook, 2019). This growth rate is in fact "much faster than the average for all other occupations".

Jobs in privacy protection and cybersecurity are not just jobs of the future but a *job sector* of the future (Armerding, 2018). In order to meet this job demand successfully, it is important to realize that not all these experts are going to perform the same task. "As is the case in most industries, it's not just a 'job' – it's a long and varied list of jobs" (Armerding, 2018). The privacy protection and cybersecurity job sector is similar to that of a good healthcare system, where there is a need for many different kinds of skilled personnel like nurses, physicians of various expertise, emergency medical responders, and medical administrative assistants, to name some. Similarly, in the privacy protection and cybersecurity field a wide range of specialists are needed like data scientists, data security analysts, secure software developers, forensic analysts, penetration testers and chief security officers (Armerding, 2018).

An important challenge presented to national and international education systems is to cope with the market demand and to deliver enough skilled workers that are capable of containing privacy and cybersecurity risks in the near future.

1.5 Approach of the research chair

The field of privacy protection and cybersecurity is concerned with the protection of (personal) information and its critical elements, including the ICT that collect, process, store, and transmit information (Whitman & Mattord, 2011).[7] An ICT-based system and the information therein are together regarded as an *Information System (IS)*. More specifically, an IS is defined as "the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources" in a setting like within an organization (Whitman & Mattord, 2011). As such, an IS is much more than just computer hardware and software.

---

7 This definition is based on the Committee on National Security Systems (CNSS) definition of "information security" (Whitman & Mattord, 2011).

The privacy protection and cybersecurity field, in general, and the realization of privacy-protecting and secure ISs, in specific, have often been characterized as a combination of art and science (Whitman & Mattord, 2011). In the field of information security, therefore, such technologists are sometimes called "security artisans" (Whitman & Mattord, 2011). Privacy protection and cybersecurity are art, as there are no concrete rules to regulate selection and configuration of various data protection and security mechanisms. Privacy protection and cybersecurity are science, as there are many sound and approved methods, techniques and guidelines to realize privacy-protecting and secure ISs. Privacy protection and cybersecurity, further, are closely related to humanities and social science, as ISs are used by people within organization, intentionally or otherwise. These users are considered as the weakest link in the chain of the measures devised and used for protecting privacy and securing ISs. Therefore, system designers, implementers and administrators should understand users' behavior in their societal and organizational context.

This field of protecting ISs against privacy and cybersecurity risks has a wide scope and covers various topics, which can be approached from different directions of, for example, individual (scientific) disciplines, system operation lifecycle/process, and system development lifecycle/process. The privacy protection and cybersecurity field can be approached from *an individual discipline*. For example, cryptography is a technological and scientific discipline that aims at developing protocols and algorithms for protecting sensitive information via hiding and preserving data integrity and authenticity. Another discipline is criminology that aims at investigating cybercrime and its criminological characteristics and impacts on victims. Ethics or law disciplines investigate which course and actions are better or necessary, respectively, to be taken in order to make use of data responsibly.

From the *viewpoint of system operation*, the aim is to protect ISs while they are in use. This protection requires dealing with privacy and cybersecurity attacks (like identifying some sensitive personal information items or sending a phishing email) before, during and after the attack. A relevant topic here is *risk management*, which is defined as the "*process* of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost" (Department of Homeland Security, 2010). A risk is defined as "the *potential* for an unwanted outcome, resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences" (Department of Homeland Security, 2010). The process of risk management addresses (a) vulnerabilities via prevention, protection and pre-event mitigation, and (b) the consequences of those events by post-event mitigation, response and recovery (Petit et al., 2013). A closely relevant topic here is *resilience*, defined as: "the *ability* of an entity — asset, organization, community, region — to anticipate,

resist, absorb, respond to, adapt to, and recover from a disturbance" (Department of Homeland Security, 2010). In the field of privacy protection and cybersecurity, the disturbance or event is an attack on privacy in or on security of an IS.

From the *viewpoint of system development*, the aim is to realize and implement ISs. To this end, a methodology is needed to guide and direct the practices. In a System Development Life Cycle (SDLC), there are a number of phases such as: Investigation, analysis, logical design, physical design, implementation, and maintenance. An example of a SLDC methodology is the waterfall model, where one goes through these phases sequentially such that the input of one phase is the output of the previous one. For implementing an IS, it may be necessary to iterate the development cycle. For realizing a privacy-protecting[8] and secure[9] IS, the privacy and cybersecurity issues of both the IS itself and the information it collects, uses and shares should be considered.

The Research Chair on Privacy & Cybersecurity (RCP&C) at RUAS, will focus on and adopt the last direction, namely the system development viewpoint, to approach the field of privacy protection and cybersecurity. In other words,

> *realizing privacy-protecting and secure ISs in practice is going to be the main mission of this research chair in the coming years.*

Achieving this objective is not straightforward as it requires making trade-offs on many fronts, such as privacy versus security (e.g., in order to deliver a certain level of security how much privacy of individuals should be compromised?), data utility versus data privacy (e.g., in order to have a good recommendation service, how much of privacy should be compromised?), and data subjects[10] being in control versus ease of use (e.g., how much of burden should data subjects be subjected to so that they can directly control the privacy protection settings themselves?). According to many scholars, real innovation is about finding a balance among contending values. Looking for such a balance shapes the mission of the RCP&C. Accomplishing this mission will be based on performing practice-oriented and/or applied-research, while striving to embed the research results in the educational curricula at RUAS.

---

8 Note that the term 'privacy-protecting ISs' refers to those ISs that are realized with privacy enhancing characteristics and capabilities. The term includes, but is not limited to, privacy protection ISs.

9 Note that the term 'secure ISs' refers to those ISs that are realized with security enhancing characteristics and capabilities. The term includes, but is not limited to, security ISs. For developing security ISs, there is a methodology called Security Systems Development Life Cycle (SecSDLC), where "the same phases used in the traditional SDLC can be adapted to support the implementation of an information security project" (Whitman & Mattord, 2011).

10 Data subject is an identified or identifiable natural person to whom personal data refer to.

Note that adopting the system development viewpoint by the RCP&C does not mean that the other viewpoints are less relevant in the field of privacy protection and cybersecurity. On the contrary, effective system development requires having inputs from various disciplines as well as considering system operation aspects as requirements, constraints and guidelines for the systems to be developed. Furthermore, note that approaching the privacy protection and cybersecurity field from the system development direction is aligned more with the guiding principles of privacy by design and security by design, as being advocating by many experts, policymakers and regulations currently.

1.6 Scope and outline of this contribution

As a starting point of the research chair's work, this contribution elaborates on a number of the shortcomings and challenges that exist in realizing privacy-protecting and secure ISs. In this contribution these challenges are denoted by the g*aps that exists between the current situation and the desired situation*. In particular, in realizing privacy-protecting and secure ISs the gap between high-level non-technological – e.g., ethical, legal, social and economic – aspects with technological aspects needs to be bridged. To this end, this contribution describes, among others, the interplay between privacy protection and cybersecurity. Further, it elaborates upon the need for applying both design-thinking and engineering approaches in order to bridge the gap between the solution space (which comprises technological and non-technological data protection and security measures) and the problem space (which comprises high-level requirements stemming from, e.g., law, ethics, economy and politics). Bridging the mentioned gaps requires further practice-oriented and/or applied-research as well as embodiment of the research results in educational curricula in the future. Therefore, by explaining the exiting gaps, this contribution portrays the research activities of the RCP&C in the coming years.

The rest of this contribution is organized as follows. An insight in privacy protection, mainly from the legal and technological perspectives, is presented in Chapter 2. Subsequently, an insight in cybersecurity, mainly as perceived from the viewpoint of developing secure ISs, is presented in Chapter 3. Both Chapters 2 and 3 elaborate also on a number of existing challenges (i.e., the gaps between the current and the desired situations). A range of approaches for designing privacy-protecting and secure ISs in socio-technological settings are sketched in Chapter 4. The design approaches described in Chapter 4 are rooted in engineering and design-thinking disciplines. Subsequently in Chapter 5, our vision is depicted on the scope of research within the Universities of Applied Sciences (UASs)[11] and how the research results can be embedded in education

11 The term UASs refers to 'hoger beroepsonderwijs (hbo) instellingen' in Dutch.

within the UASs. Finally, the main conclusions together with near future research focus of the RCP&C are presented in Chapter 6.

Privacy protection

This chapter provides an insight in privacy protection mainly from the legal and technological perspectives. To start with, it is worthwhile to note that the term privacy is not used in the new EU GDPR. This is because the scope of privacy is wide and includes also non-data-related aspects like physical privacy (Verheul et al., 2016). Not using the term privacy within GDPR is due to the fact that the regulation is concerned with personal data protection. Similarly, our scope is the data related aspects of privacy. Nevertheless, we use the term privacy because of the breadth of the material and understandings that are based on it.

This chapter starts with a brief introduction to the evolution of privacy concept (Section 2.1). As a baseline for our system development approach, a framework for conceptualizing privacy is presented subsequently (Section 2.2). To indicate the status of current approaches for privacy protection, the privacy principles adopted in the legal domain and the technological strategies derived from these principles are presented in Sections 2.3. Section 2.4 highlights the fact that privacy protection is a process and that privacy by design is the key for realizing privacy protection. Sections 2.3 and 2.4, moreover, point out the existing gaps[12] between technological and non-technological data protection measures, and between both of these measures and the high-level privacy requirements. Subsequently, Section 2.5 will elaborate on existing gap between the definitions of privacy in legal and technological domains, and the future directions to address this gap in practice. Finally, the key results of this chapter are summarized in Section 2.6.

2.1 On the concept of privacy

Privacy is a normative concept that is deeply rooted in various disciplines such as philosophy, law, ethics, politics and sociology (Nissim & Wood, 2018a). Many efforts have been put to conceptualize privacy (i.e., to define what privacy is, what makes it unique and distinct) by searching for a common set of necessary and sufficient elements that single out privacy as unique from other conceptions (Solove, 2008). This section briefly describes the evolution of the concept of privacy, particularly in the course of technological developments as much as possible.

Aristotle made distinction between public and private spheres of life, which is seen as the early principled discussion of privacy (Nissim & Wood, 2018a). Since then, many definitions for privacy have been introduced, particularly within legal regimes. In the following, as representative examples, four privacy definitions and their deficiencies are summarized from (Solove, 2008).

12 Some directions on how to bridge this gap will be presented in Chapter 4.

1. *The right to be let alone*: At the end of the 19th century Kodak's new snap cameras, which enabled anybody to take instantaneous pictures of others, and widespread newspaper circulation motivated Warren and Brandeis (1890) to define privacy as *to lives one's life as one chooses, free from assault intrusion or invasion*. This definition does not give much guidance about what privacy is and on what matters one should be let alone.
2. *Limited access to the self:* About the same time as Warren and Brandeis, Godkin (1880) considered privacy as *the right of every man to keep his affairs to himself and to decide what extent of these affairs shall be the subject of public observation and discussion.* This view on privacy does not provide much guidance about, for example, what these private matters are and the degree of access.
3. Secrecy: As a common understanding of privacy, this view considers that *privacy is violated by the public disclosure of previously concealed information*. This view, which is a specific case of limited access to oneself, is too narrow and, for example, fails to recognize group privacy (i.e., sharing personal information within groups, which is not secret anymore but is still private) and fails to recognize data usage control aspects.
4. *Control over personal information*: As a predominant theory of privacy, like some other scholars, Westin (1968) defines privacy as *the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*. This view, in the realm of data related privacy, is too broad as, for example, it does not specify the types of personal information and what the control is.

Solove also elaborates on the shortcomings of two other definitions of privacy, namely: Personality integrity (i.e., protection of personhood) and control over intimacy (i.e., control over developing personal relationships like love, caring and loving). These definitions are not elaborated upon here anymore for brevity purposes, the interested reader is referred to (Solove, 2008) for further information. Based on this analysis, Solove argues that these privacy concepts are either over inclusive (too vague) or too restrictive. Subsequently, Solove concludes that privacy cannot be conceptualized in a definition with some necessary and sufficient conditions (i.e., based on inclusion and/or exclusion rules).

Defining privacy is an attempt to generalize the concept of privacy. But this generalization, unlike the definitions discussed above, should be done at the right abstraction level. Contextualization of privacy is another move in the opposite direction of generalization to achieve pragmatism. A major step towards contextualization of privacy is taken by Nissenbaum (2004) who considers contextual integrity as the benchmark of privacy. According to Nissenbaum's contextual integrity, privacy is infringed when one or more information norms are

violated in a given situation (i.e., the normative expectations about the appropriate flow of information are violated). "These information norms are of two types: appropriateness, which governs *what* information about persons is appropriate to reveal in a given context, and flow or distribution, which governs *how far* information about persons is transferred in a given context" (Bargh, Choenni & Meijer, 2016). The context is a sphere in which the information is shared. The sphere, in turn, captures the whole environment including the audience, location, politics, culture and so on.

It is interesting to acknowledge the role of technological developments in the evolution of privacy definitions. Th definition of Warren and Brandeis, i.e., the right to be let alone, came up in a critical reaction to Kodak's new snap cameras and widespread newspaper circulation more than a century ago. Later on, the role of ICT developments in the late 1970's can be traced in Westin's definition (1968), i.e., control over personal information. In current digital world, with personal computers, smart mobile devices and IoT devices, privacy is not a sole issue of journalism and publishing anymore, but it has been intertwined with almost every activity of individuals due to the widespread adoption and ubiquitous deployment of ICT, see (Choenni et al., 2011b).

2.2 A reference model for privacy protection

Although it is necessary to look at the contextual aspects in protecting privacy, there is a need for a framework (or theory) at an appropriately generic level that guides the privacy protection process (Solove, 2008). After all, addressing privacy protection purely based on contextual aspects and exceptions may not give sufficient direction for making legal judgements and for policymaking. Solove (2008) suggests adopting a pluralistic approach based on *family resemblance* theory of Wittgenstein (2009). According to this theory, a set of overlapping, but not identical (i.e., exactly defined) features link the members of a group (e.g., the members of a family have resemblance to each other, considering the forms of their eyes, gait, face, body, etc. combined). Inspired by the theory of family resemblance, Solove suggests a framework to resurface the harmful impacts of data related activities on privacy (i.e., privacy risks[13]) via a bottom up approach, rather than based on what the privacy definition is.

13 Solove uses the term 'privacy problem' instead of the term 'privacy risk' used here. One can also use terms such as 'privacy threat' or 'privacy harm'. Throughout this contribution the term 'privacy risk' is used for having a harmonious presentation. Note that, in a more technical sense, these terms differ slightly and are not exactly the same.

Solove's framework, illustrated in Figure 1, aims at identifying possible privacy risks in four steps within a typical data analytics process, namely:

1. Data collection, via which privacy risks can be inflicted even if nothing is revealed about individuals,
2. Data processing, which includes various operations like data linkage, data analytics, data storage, and data usage. Via data processing even it is possible to create new personal information,
3. Data dissemination, via which the processed personal data are spread and shared with others,
4. Invasion, via which the lives of people are affected adversely, noting that the impacts are not always in cyberspace (i.e., can cause physical harms)[14].

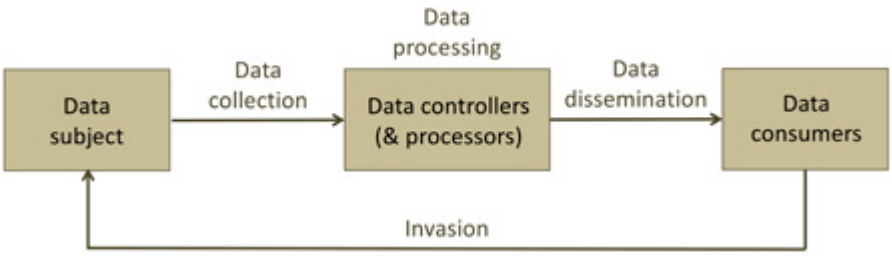


Figure 1: A modified version of Solove's mode (adopted with adaptions from Solove, 2008).

Per each step of the framework, one can identify a number of privacy risks, as summarized from (Solove, 2008) in Figure 2 and the adverse impacts that limit liberty, autonomy and income of individuals from (Crawford & Schultz, 2014). Note that these privacy risks are not exhaustive and can be extended and expanded per case and context. For descriptions and definitions of the privacy risks shown in Figure 2 the interested reader is referred to (Solove, 2008).

14 ÐIn Section 2.5 a new trend for defining privacy is described, which pleas for a formal definition of privacy that is soundly implementable.

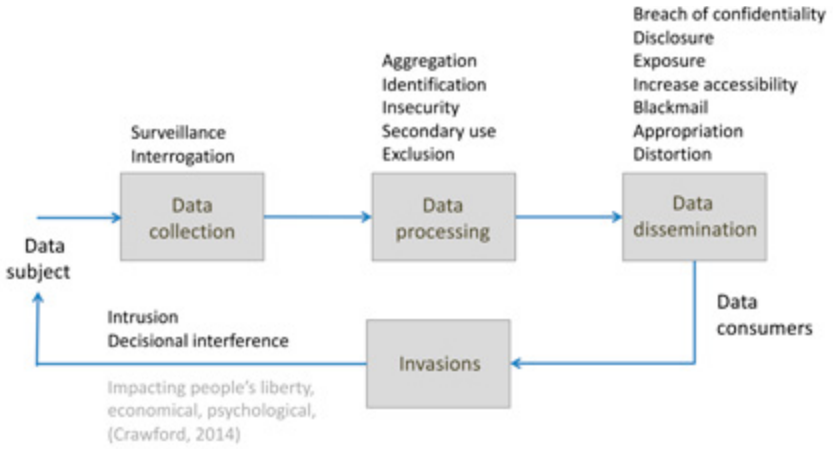


Figure 2: A modified version of Solove's model of privacy risks (adopted with adaptions from Solove, 2008).

We find Solove's framework intuitive within the domain of data analytics, Artificial Intelligence (AI), and data-driven applications. It is intuitive in the sense that it captures the data lifecycle in these domains, whereby privacy risks can be associated to each step of the data lifecycle systematically. This data lifecycle also resembles a typical System Development Life Cycle (SDLC), whether the IS (to be) developed is concerned with collecting, analyzing and sharing data from some sources, for a purpose, via a hardware and software platform, and within an organizational/environmental context. As an example, in (Harbers et al., 2019) such a model has been used as a boundary object (Star & Griesemer, 1989; Star, 2010) in the design process of an IS in order to enhance the understanding of stakeholders in the early stages of a privacy by design process.

In addition to using Solove's model in the SDLC of an IS (to be) developed, one can use this privacy risk model within a risk management process to identify the privacy risks within an existing IS and to devise mitigation measures for high privacy risks (i.e., to carry out privacy by redesign).

2.3 Privacy protection in practice

In order to indicate the current status of privacy protection in the *technological domain*, this section presents a number of well-known technological strategies for privacy protection. These strategies can straightforwardly be translated to implementable techniques, protocols and algorithms. These strategies, in turn, are based on the privacy principles embedded in current privacy laws and regulations. Therefore, the section first provides an overview of these privacy principles in legal regimes (Subsection 2.3.1), followed by a description of the technological strategies (Subsection 2.3.2).

2.3.1 Legal principles of privacy protection

In current data privacy laws and regulations, the notion of identifying or personal information has played a central role.[15] Note that personal information is defined differently across sectors, jurisdictions and contexts. Some regulations define it narrowly[16] and some define it broadly (Nissim & Wood, 2018a). The EU's GDPR provides a generic definition of personal data/information, as any information that relates to an identified or identifiable natural person (so-called *data subject*). Specifically, "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person", see Article 4 of GDPR (2016).

Within a specific data privacy law or regulation, the information that is regarded as personal information should generally be protected. Within GDPR, for example, Article 5 mentions the following principles for privacy protection.

- *Lawfulness, fairness and transparency principle*: Specifying how the data should be processed in relation to data subjects,
- *Purpose limitation principle*: Specifying that personal data may only be collected for specified, explicit and legitimate purposes and not further be processed in a manner that is incompatible with those purposes,
- *Data minimization principle*: Specifying that personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected and processed,
- *Data accuracy principle*: Specifying that data should be accurate and, where necessary, kept up to date. Hereto, every reasonable step must be taken to ensure that personal data that are inaccurate, given the data purposes at hand, are erased or rectified without delay,
- *Storage limitation principle*: Specifying that data should be kept in a form that the identification of data subjects is possible only for the interval necessary for the specific purpose in mind and no longer,[17]
- *Integrity and confidentiality principle*: Specifying that data should be secured appropriately; the data must be protected against (accidental) loss, destruction or damage as well as be kept confidential against unauthorized or unlawful access and processing, and
- *Accountability principle*: The data controller[18] shall be responsible for the abovementioned principles and should demonstrate his/her compliance with those principles.

---

15 In section 2.5 a new trend for defining privacy is described, which pleas for a formal definition of privacy that is soundly implementable.

16 Like Massachusetts data security regulation, see Nissim and Wood (2018a).

17 Except for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

18 A data controller is a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Article 4(7) of GDPR, 2016).

In addition to abovementioned principles, putting data subjects in control of their personal data is also emphasized in GDPR. According to Article 6, data processing is lawful if the subject has freely given consent[19] to processing her/his data. Note that the provision of a service should not be conditional on giving consent if the processing of the personal data is not necessary for the performance of that contract, see Article 7 (4) of GDPR. For example, a social network provider called Alice.com cannot oblige a service consumer called Bob (being also the data subject) to give consent for collecting Bob's location (i.e., Bob's personal information) by Alice.com, as a precondition of using the service by Bob, unless Bob's location is necessary for the service provisioning. The data subject has the right to transparency about, to access to, to rectification of, to erasure of, to restriction of the use of, and to portability of her/his personal data, see Articles 12-22.[20] The right to transparency about personal data, for example, means the data subject should be informed if her/his personal data are collected and processed. Further, the data subject has the right to object any automated decision making, see Articles 21 and 22.

It is worthwhile to note that the abovementioned data protection principles stem from those suggested by the Organization for Economic Co-operation and Development (OECD). The OECD is an intergovernmental economic organization, founded in 1960, to stimulate economic progress and world trade. It is a forum for countries committed to democracy and the market economy via "establishing international norms and finding evidence-based solutions to a range of social, economic and environmental challenges".[21] The forum offers a knowledge hub "for data and analysis, exchange of experiences, best-practice sharing, and advice on public policies and global standard-setting". The OECD privacy principles were previously adopted by the European Commission (EC) Data Protection Directive (Directive 95/46/EC), which proceeded the current GDPR.

2.3.2 Technological strategies for privacy protection

Using the data protection principles proposed by OECD (at the time, adopted in Directive 95/46/EC and later adopted in GDPR) as point of departure, Hoepman (2014) derived eight privacy design strategies that privacy by design architects can use early in the software development process. These privacy design strategies, which are closely tied to the technological domain techniques and methods, are summarized with some extension in the following.

---

19 There are exceptions to this, like the data processing being necessary for performing a contract, for compliance with law, for protecting vital interests of data subject, for carrying out a task in the public or legitimate interests.

20 Note that some exceptions apply.

21 See https://www.oecd.org/about/.

1. *Inform* data subjects adequately whenever their personal data is processed. Informing data subjects can be done by pushing notifications to data subjects (like sending data breach notifications to data subjects in case of privacy breaches as required in reporting obligation by (Dutch) Data Protection Authority, DPA[22]) or by pulling requests by data subjects (like the Light beam add-on for the Firefox web browser that can be consulted by data subjects to see the third party tracking cookies placed on the browser while data subjects visiting various websites).
2. *Demonstrate* the compliance with the privacy policy and any applicable legal requirements. Example systems and approaches that can serve this end are privacy management systems, logging and auditing systems, and design for accountability approach.
3. Give *control* to data subjects over the processing of their personal data. Examples are the possibility of requesting Google to erase search results and (dis)approving the use of cookies when visiting websites.
4. *Enforce* a privacy policy that is compatible with legal (and personal) requirements. This can be perceived as having control on behalf of data subjects. Examples are access control and usage control mechanisms that control the access to and the use of resources (like personal data), respectively (Bargh, Vink & Choenni, 2017b; 2018b). Another example would be having a button to erase personal data, thus realizing the right-to-be-forgotten principle.
5. *Minimize* the amount of personal data to be processed. An example is the selection of the relevant attributes before collecting/sharing data.
6. *Aggregate* personal data at the highest level with the least possible detail in which they are still useful (i.e., making the so-called data utility-privacy trade-off). An example technique is the generalization of attribute values before processing them. For example, Statistical Disclosure Control (SDC) methods (Bargh et al. 2018) can be used to generalize the age attribute (e.g., instead of sharing the exact age attribute values, share the age values in 5 years intervals).
7. *Hide* any personal data and their interrelationships from plain view. Hiding can be done by, for example, data encryption to change a plain text to a cypher text that is unreadable for unauthorized persons: Only authorized persons who have a decryption key can transform the cypher text to the original plain text and hereby the original text is hidden for unauthorized persons. Another technique is the TrackMeNot browser plugin for the Firefox web browser that obfuscates users searches via periodically issuing randomized and meaningless search-queries to popular search engines.[23]

---

22 (Dutch) Data Protection Authority (in Dutch: Autoriteit Persoonsgegevens), see https://autoriteitpersoonsgegevens.nl.

23 See https://cs.nyu.edu/trackmenot/.

8. *Separate* personal data and process them in a distributed way whenever possible. For example, data pertaining to Bob, a student at RUAS, are spread in various data centers at RUAS. For a more complex example, data anatomization is an SDC method to split a dataset to multiple datasets, while being able to have some statistical analyses without being able to link individual records (Fung et al., 2010).

2.3.3 Applying technological strategies to practice

In a SDLC the technological strategies are ingredient components used within the design, physical design and implementation phases to *implement* the technological parts of privacy-protecting ISs. In practice, however, privacy requirements should be derived according to, for example, Solove model shown in Figure 1 and Figure 2. Part[24] of these privacy requirements can be mapped to these technological strategies, which in turn can be realized within engineering domain with Privacy Enhancing Technologies (PETs) in hardware and/or software. In practice, therefore, it is necessary to have or devise a process (or an iterative process) for

a. Deriving high-level privacy related legal, ethical, societal, etc. requirements (see Sections 2.2 and 2.3.1) and
b. Translating (part of) these high-level requirements to a set of privacy strategies that, in turn, can be implemented with PETs, see Subsection 2.3.2.

Although there are some work done in the field of (privacy) requirement engineering,[25] there is no well-stablished and systematic process, or design methodology, to bridge the gap between, on the one hand, the technological strategies (and techniques) and, on the other hand, the high-level and context-dependent privacy requirements. This need is symbolically illustrated with a gap in Figure 3. (Note that, in addition to technological strategies, non-technological strategies are needed to realize privacy requirements in practice. Finding a good balance between technological and non-technological strategies is another challenge in designing privacy-protecting ISs. This challenge is also indicated on the left side of Figure 3).[26]

---

24 For the other part, non-technological measures might be needed (like organizational procedures, social/professional protocols, educational campaigns and contracts).

25 See Section 4.1 for an overview.

26 As the focus of the research chair (i.e., RCP&C) is more on bridging between technological strategies and high-level privacy requirements, non-technological privacy protection measures are set on the side-track in this section. By no means implies this choice of presentation that technological measures are more important than the others. In the following (sub)sections, there will be no strict separation between these technological and non-technological measures of privacy protection.

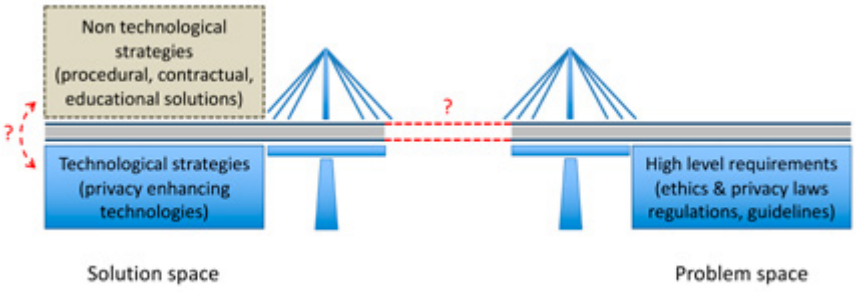


Figure 3: An illustration of the existing gap between the technological domain (or privacy engineering domain) and the high-level privacy requirement domain (stemming from legal, ethical, social, etc., domains).

2.4 Privacy by design

In developing new ISs, the principle of privacy by design pleas for filling the gap between, on the one hand, technological and non-technological data protection measures (where the former can be related to the technological strategies used in the previous section) and, on the other hand, the high-level (and probably, undiscovered) privacy requirements. One of the pioneering advocates of privacy by design is the Canadian privacy commissioner Ann Cavoukian who laid down the initial sub-principles of privacy by design as follows (Cavoukian, 2010):

1. Being proactive not reactive through devising preventative not remedial measures,
2. Considering privacy as the default setting,
3. Embedding privacy into design and architecture,
4. Providing full functionality, according to which privacy does not come in cost of other functionalities (i.e., attaining the positive-sum, not the zero-sum),
5. Providing end-to-end security, whereby the full lifecycle of data is protected, from cradle to grave,
6. Keeping it open and transparent, whereby all stakeholders can be assured through independent verification, and
7. Being user-centric, whereby user privacy is respected by keeping the interests of the individual uppermost.

These privacy by design sub-principles do not provide practical guidelines about how to design ISs in practice. Some of these sub-principles are even perceived as inconsistent (Bier et al., 2012). For example, Bier et al. (2012) discuss the shortcomings of these principles and propose some refinements and enhancements to make them more consistent and pragmatic. Nevertheless, the initiative of Cavoukian has been instrumental in awakening all parties and stakeholders involved (like policymakers, legislators, system architects and developers, data subjects, data controllers, and data processors) to take the

subject matter into consideration seriously. As off today, privacy by design has become one of the key bases of GDPR for data protection (among other data protection principles, concepts, methodologies and technologies), see Article 47(d) of GDPR. In case of high privacy risks, GDPR also asks for executing a Data Protection Impact Assessment (DPIA), which can be seen as a blueprint of a high-level design, established in early stage of any personal data processing endeavor.

Inconsistency in privacy by design sub-principles is inevitable as the IS designer is concerned with a socio-technological setting and context (Mumford, 2006), where many trade-offs should be made among contending values and objectives. As creating a formal model of such settings is not always possible, applying conventional engineering design methods is not always possible. We believe a methodology based on design-thinking and conventional design within engineering is needed that, as two complementary components, realize the privacy by design principle systematically, as envisioned within GDPR. This complementary approach is symbolically illustrated in Figure 4 as a bridge to link the gap between technological and non-technological[27] data protection measures (i.e., the so-called solution space) and the high-level (and probably hidden) privacy requirements (i.e., the so-called problem space). In Chapter 4 there will be more elaboration on such a complementary approach for privacy by design.

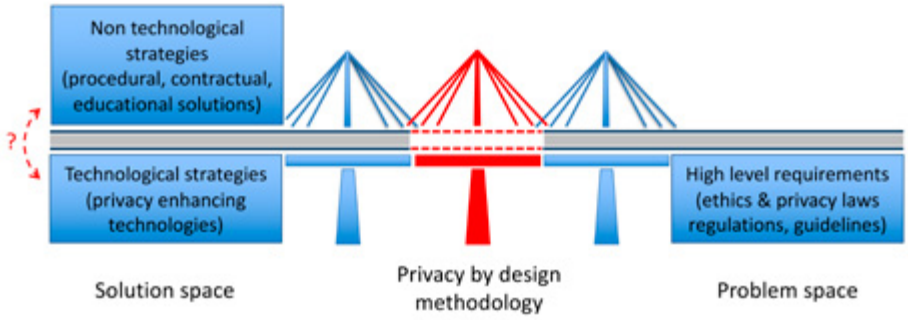


Figure 4: Privacy by design methodologies to bridge the gap between the solution and problem spaces.

27 Note that, unlike Subsection 3.3.3 that focuses on technological privacy protection measures, this subsection considers also non-technological privacy protection measures like organizational procedures, social protocols, educational training, and contracts.

2.5 Trends and developments

Current legal regimes and most definitions of privacy are based on the *normative* and intuitive assumptions "about how pieces of information interact, rather than (and often contradicting) scientific and mathematical principles" (Nissim & Wood, 2018a). For example, GDPR defines anonymous information as the "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" (see Recital 26 of GDPR). According to GDPR, the rest is considered as personal information. In order to determine the possibility of a natural person being identifiable, one must consider "all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments", see Recital 26 of GDPR.

Therefore, according to GDPR, the anonymity (or identifiability) of data is determined normatively, in relation to other datasets and environment conditions. Bargh et al. (2018; 2019) argue that data anonymity in the GDPR sense can be achieved if the data disclosure risks are contained within an acceptably negligible level, considering, among others, available technologies, other data sources, and the costs of re-identification at the time of data anonymisation. Note that data disclosure risks may increase over time due to availability of other datasets and changing environment conditions. Thus, the currently anonymous data may become personal data in the future (WP29, 2014). This implies that an applied privacy protection mechanism, which results in an anonymous data set currently, may not do so in the future. The concept of contextual integrity of Nissenbaum (2004) is another way of approaching privacy in a normative way. It assumes that privacy breaches can be tracked when information flows in a particular context violates societal norms. In other words, the contextual integrity approach assumes that the norms can be defined formally, i.e., in an unambiguous and effectively testable way.

The argument mentioned above on anonymity according to GDPR indicates that the normative approach for privacy is based on induction, which can be expressed by the metaphor of all swans are white unless a black one is discovered (e.g., an anonymized dataset is anonymous unless it is re-identified). Nissim and Wood (2018a) conclude that

> *"[n]ormative concepts are often not defined explicitly, and, when they are, they are not expressed in a formal language that enables a precise analysis. As a result, there is uncertainty with respect to which information flows are in agreement with normative concepts. In many cases, it may be difficult to determine with reasonable certainty whether an information flow is appropriate, whether it creates a risk of a privacy breach, or even whether a privacy breach has in fact occurred."*

There are a number of gaps in realizing privacy-protecting ISs in regard to linking current privacy related legal regimes and elucidating the ethical and legal requirements and definitions. Some of these gaps, according to Nissim and Wood (2018a), are between:

a. The privacy concepts in real-life (rooted in ethics, sociology, culture, ...) and their implementation in current normative legal concepts (i.e., in privacy laws).
b. The current normative concepts of privacy in different cultures, jurisdictions and disciplines. This gap, among others, makes it challenging to protect privacy in cross domain and trans-jurisdiction flow of personal data.
c. The normative legal concepts of privacy and the technological concepts of privacy, as discussed in this section and illustrated in Figure 3. This gap introduces challenges in applying PETs in practice.

Bridging gap (a) is a huge task in legal domain purely, thus it is out of the scope of the RCP&C. The RCP&C is going to adopt a systematic privacy by design approach, see Chapter 4 and Section 2.4, which, we believe, is a way forward in eliciting and elucidating technological, ethical, cultural, political, etc. requirements of privacy and realizing them using technological and procedural measures. Thus, we will focus on addressing part of gaps (b) and (c).

For gap (c) we currently see an interesting trend in a specific area of privacy protection, namely, technological approaches for protecting privacy in statistical computation and the normative notions of de-identification and anonymization underlying many privacy regulations. This trend is to move from the current normative legal concepts of privacy to the formal legal concepts of privacy. Formal privacy models are based on mathematically and rigorously proven techniques such as differential privacy (Dwork, 2006). Unlike normative approaches to privacy, these formal models are not subject to interpretation in different contexts inherently. Normative concepts, which are embedded in existing regulations and laws like GDPR, often rely on intuitive assumptions about how pieces of information interact, rather than the properties of a data set itself which can be examined by scientific and mathematical principles. To illustrate this, consider the following examples.

According to the normative notions of de-identification and anonymization which underlie many privacy regulations including GDPR, a given dataset D is personal data if it can reveal personal information when it is combined with other datasets D′ available to legitimate and illegitimate data recipients (i.e., the privacy intruders). Datasets D′ are called background information. In revealing personal information, the amount of the contribution of dataset D relative to that of datasets D′ is not considered in current normative models. The amounts of the contribution of dataset D relative to that of datasets D′ are shown schematically in Figure 5 (specially, consider three example cases I, II and III therein). The more one moves towards the right direction, the contribution of data set D (i.e., the blue part) decreases while that of the background information (i.e., data sets D′ indicated by the gray part) increases. As illustrated in Figure 5, there are clear differences in the ratios of contributions for Case I and Case II. Also shown in Figure 5 is Case III, where the collective impact of data set D and data sets D′ does not lead to disclosure of personal information, because the sum of the two parts is below the dotted threshold value. Should the amount of background increase in the future, then dataset D in Case III can be regarded as non-anonymous at that time.

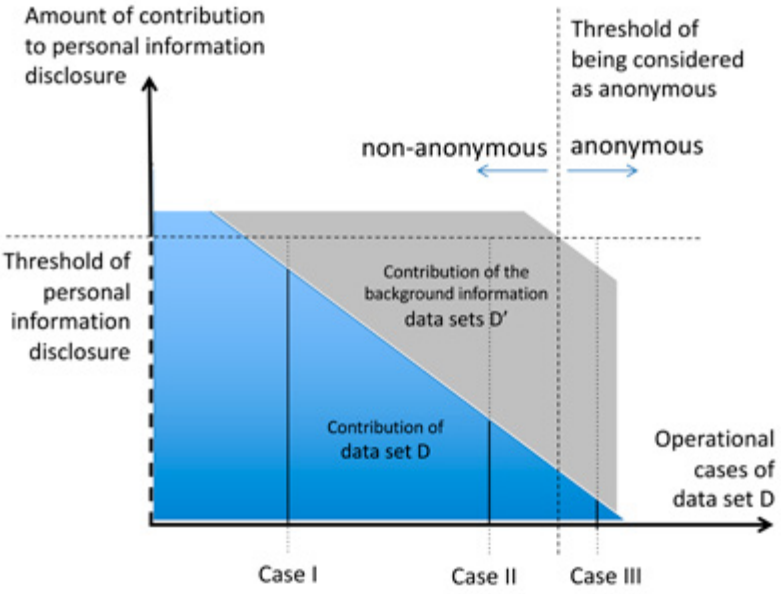


Figure 5: An illustration of the amount of contribution of data set D to disclosure of personal information.

Dwork et al. (2006) showed that it is impossible to enforce the stringent definition of privacy protection, as proposed by the current normative definitions, when the intruder has an arbitrary amount of background knowledge. Bargh at al. (2018a) mention the following example about the impact of background knowledge, which is adopted from (Dwork et al., 2006).

> *"Suppose that individuals' age is sensitive information. Further assume that, as background knowledge, an intruder knows Alice's age is five years younger than the average age of American women. If we disseminate a microdata set about the ages of American women, then the intruder can calculate the average age of American women from the released microdata set and infer Alice's age. According to current definitions, the 'release of the microdata set' has violated Alice's privacy (even if Alice is not American and thus her record is not in the released data set)."*

This example shows that background knowledge may have a more dominant role in revealing someone's personal information than a specific dataset does, see case II in Figure 5. Therefore, framing privacy in normative ways can result in expressions of unrealistic privacy desiderata, leading practitioners towards pursuing an idealized privacy goal that is impossible to achieve (Nissim & Wood, 2018a).

Therefore, Dwork et al. (2006) provided a new definition of privacy when introducing their differential privacy technique. According to this definition, *the presence or absence of the (personal) data of an individual* in a dataset must not have an observable impact on the output of an analysis/computation over that data set. In other words, it requires that "the output distribution of a privacy preserving analysis to remain stable under any possible change to a single individual's information" (Nissim & Wood, 2018a). One can refer to Nissim et al. (2018b) for a more detailed discussion of how differential privacy protects data.

It is worthwhile to mention that the technique of differential privacy that realizes the definition mentioned in the previous paragraph is already in use in many current systems and data sharing by, for example, Google, Apple, Uber, and the U.S. Census Bureau.
Apple uses the technique in iOS10 for increasing its security and privacy[28], Google uses it for protecting urban mobility data to ensure individual users and journeys cannot be identified[29], and the U.S. Census Bureau wants to apply it to 2020 US census data to safeguard the information it gathers from the public[30].

Nissim et al. (2018b; 2018c) argue that it is important to have a rigorously provable formal definition of privacy that can be realized technologically irrespective of all contextual and environmental conditions. Having considered the formal definition of differential privacy, they *advocate instrumenting the law with such a modern scientific understanding of privacy, and even guiding the development of modern conceptions of privacy in the law*. This approach actually relies on a deduction-based reasoning for privacy laws and regulations, whereby the development and implementation of new privacy technologies demonstrably adhere to legal requirements for privacy protection. According to a deduction-based reasoning, one can conclude that a specific swan is a bird based on the assumption/rule that all swans are birds. This approach could be instrumental to bridge the gap between the legal and technological domains of privacy, whereby privacy legal desiderata can more closely be matched with today's large number of information sources available as background information (i.e., the so-called big data). Adopting such laws and using such techniques can be future proof and robust against unknown future privacy attacks (Nissim et al., 2018c).

---

28 See https://www.apple.com/newsroom/2016/06/apple-previews-ios-10-biggest-ios-release-ever/
29 See https://europe.googleblog.com/2015/11/tackling-urban-mobility-with-technology.html.
30 See https://www.census.gov/newsroom/blogs/random-samplings/2019/02/census_bureau_adopts.html

2.6 Conclusion

This chapter provided an insight in privacy protection, mainly from the legal and technological perspectives. After describing a number of privacy definitions, it concluded that privacy cannot be conceptualized in a definition with some necessary and sufficient conditions. Instead of defining privacy, identifying privacy risks in an IS is needed in practice. To this end, a model is presented from literature for conceptualizing privacy at a right abstraction level and, eventually, for guiding any privacy protection process.

After describing the current legal principles of privacy and the technological strategies of privacy protection, it is argued that there is a gap between high-level legal requirements and technological strategies, which needs to be bridged in the future research. Privacy protection asks for adopting a privacy by design methodology that links the gap between solution space (i.e., technological and non-technological (e.g., procedural, educational and contractual) measures) and the problem space (i.e., high-level design requirements).

Finally, a current trend is elaborated on that aims at bridging the gap between the normative definition of privacy, as adopted already in privacy laws and regulations, and the need for a formal definition of privacy, as ideally required for realizing sound technological solutions. The rise of this trend is interesting as it reconfirms

the historical evolution of the concept of privacy with technological developments.

Cybersecurity

This chapter provides an insight in cybersecurity, mainly as perceived from the viewpoint of developing secure ISs. Cybersecurity focuses on securing digital assets. These assets turn around data and the infrastructure that creates, transports, processes and stores data. As such, the field of cybersecurity covers protection of the communication, processing and storage equipment as well. To start with, it is worthwhile to note that the term cybersecurity and information security are considered and used as synonym in this contribution. Nevertheless, we use the term cybersecurity more often relatively because the term has been adopted within RUAS more widely as well as been part of the title of this research chair.

This chapter starts with a brief introduction to the concept of cybersecurity and its evolution (Section 3.1). As a baseline, a framework for conceptualizing cybersecurity is presented based on the critical characteristics of information relevant for cybersecurity (Section 3.2). To highlight its importance, security by design is elaborate upon in Section 3.3. The interplay between privacy protection and cybersecurity is explained in Section 3.4. Subsequently, the issues of cybersecurity (and privacy protection) in complex and distrusted ISs are elaborated upon in the context of safeguarding the IoT in Section 3.5. Sections 3.4 and 3.5, moreover, point out the existing gaps between privacy protection and cybersecurity, and between the current situation and the need for adopting a holistic approach for addressing the cybersecurity (and privacy) issues of complex and distrusted ISs. Finally, the key results of this chapter are summarized in Section 3.6.

3.1 Evolution of cybersecurity

An interesting introduction to the history of information security is given by Whitman & Mattord (2011). In the following, a summary of this introduction is presented in the context of the progresses made in computing in recent years.

Information security began with *computer security* during World War II, when the first mainframes were developed to break secret communication codes. In these early times, computer security was a straightforward process, mainly limited to physical security and simple document classification. Physical theft of equipment, espionage against systems, and sabotage were the primary security risks of computer systems.

During the Cold War (i.e., in the 1960s), computing specialists wanted to carry out more complex and sophisticated tasks and, therefore, it was necessary to exchange data among mainframes at different computer centers. As a result, mainframes were made online to communicate their data. In this way, the exchange of data became more effective than mailing magnetic tapes between computer centers. To enable the exchange of data, the Advanced Research Project Agency (ARPA) of the US Department of Defense developed a networked communication system for the military. The outcome was ARPANET, which is considered as the predecessor to the Internet. During the 1970s and 1980s, as ARPANET became popular and was used more widely, some vulnerabilities of ARPANET were identified, for example, lack of adequate safeguards against unauthorized remote users, vulnerability of password structure and formats, and lack of safety procedures for dial-up connections. Due to rise of such computer security violations in ARPANET, *network security* prevailed. Nowadays, network security deals with, for example, protecting WiFi as a typical wireless network. Meanwhile, a famous study in 1978 brought up the importance of *operating system security*. Today, operating system security deals with securing, for example, Windows, Android and OSi.

With the advent of the microprocessor in the late 1970s, Personal Computers (PCs) moved computing out of data centers. As another new age for computing, decentralization of data processing systems in the 1980s led to interconnecting PCs and mainframe computers, enabling resource-sharing and collaboration within computing community. As networks of computers became more common in the 1990s, the Internet as the first global network of networks was born. Gradually, the Internet became available to the general public instead of being within the domain of governments, academia, and specific industries. In early stages of the Internet deployment, security had a low priority. "In fact, many of the problems that plague e-mail on the Internet today are the result of this early lack of security" (Whitman & Mattord, 2011). These security shortcomings of e-mail can be associated with the fact that, at the time, the developers of e-mail assumed the Internet and e-mail users were trustworthy computer scientists. As the early security was aimed at protecting the physical environment of data centers, the ability to secure a networked computer was weakened and, therefore, the stored information became more exposed to security threats.

Nowadays, the Internet interconnects a huge number of (unsecured) computers, smart phones, and IoT devices. It provides a medium for these devices to exchange data with each other. In such a set of interconnected devices, the security of every device is dependent on other devices. As most of these interconnected devices are insufficiently secured currently, the need to improve information security is immense more than ever. This need has become a commonplace nowadays as all parties involved (e.g., governments, citizens and companies) have felt the

importance of information security for sustaining the well-functioning of, perhaps, every aspect of the society.

3.2 Critical information characteristics

As mentioned In Section 3.1, information security was evolved from the early field of computer security. Information security, as we call it cybersecurity, according to the US Committee on National Security Systems (CNSS), is concerned with "*protection of information and its critical elements, including the ICT systems (software and hardware) that use, store, and transmit that information*" (Whitman & Mattord, 2011). Cybersecurity aims at protecting a number of the, so-called, *critical characteristics of information assets*, whether in storage, processing, or transmission. Cybersecurity is achieved via the application of policy, education, training and awareness, and technology. The traditional critical characteristics of information assets that should be protected are as follows:

- *Confidentiality*, to protect information from disclosure or exposure to unauthorized individuals or systems. For example, passwords are confidential information that should not be exposed to system administrators or the public,
- *Integrity*, to protect information so that it is whole, complete, and uncorrupted. For example, bank account information should not be modified or manipulated by criminals or due to frauds,
- *Availability*, to enable authorized entities, e.g., persons or computer systems, to have access to information without interference or obstruction, and with the required data quality. For example, a Denial of Service attack (DoS attack) is a typical cyberattack that causes a resource, e.g., someone's bank account, to become unavailable for the person. Such a DoS attack disrupts individuals' lives and banks' businesses.

The abovementioned critical information characteristics that are traditionally protected via cybersecurity are referred to as the *CIA triangle*, where the abbreviation refers to their initial letters. Due to ongoing developments of ICT and due to volatile changes within cyberspace (consider the rise of, for example, cybercrimes, new threats, disruptive technologies, and high impact applications), considering only the CIA characteristics of information assets seems no longer to be adequate for cybersecurity. Therefore, to address the risks of the constantly changing environment, new critical characteristics of information are recognized in literature and/or industry that should be protected (Whitman & Mattord, 2011). Examples of such new characteristics are as follow:

- *Accuracy*, to ensure that information is free from mistakes or errors and has the expected value. For example, the age of a person who wants to receive a service targeted for specific age groups should not be registered inaccurately, whereby the person cannot receive the service (s)he deserves, or otherwise,

- *Authenticity*, to protect the quality or state of being genuine or original, rather than a reproduction or fabrication. For example, a phishing email spoofed under the name of someone's bank is not original, while its recipient may think otherwise and might undertake undesired actions,
- *Authorization, t*o determine what can be done with information by entities (e.g., persons or computer systems). For example, a bank employee should be able to see the bank account information of customers in certain situations, e.g., for checking account balance when a customer asks for a loan, not out of own curiosity, and
- *Possession*, to maintain the state of ownership or control over information. For example, information cannot be obtained (i.e., possessed) by unauthorized individuals. Note that a breach of possession does not lead to a breach of confidentially, for example, when the disposed information is encrypted.

In the rest of this contribution the traditional CIA characteristics of information assets will be considered as they are most widely adopted in literature and industries. Extension of the discussion results to new critical information characteristics is straightforward.

3.3 Security by design

Many approaches exist for realizing secure ISs. To this end, an interesting model widely used in computer and information security is the CNSS security model, also known as the McCumber Cube named after the person who proposed the model. The CNSS security model is a graphical representation of the architectural approach for cybersecurity (Whitman & Mattord, 2011) and consists of three dimensions and three levels per dimension as follows:

1. Data analytics steps, which comprises the three steps of storage, processing and transmission,
2. Information characteristics, which comprises the three CIA characteristics (i.e., confidentiality, integrity and availability), and
3. Security controls measures to protect information assets, which comprises the three measures of policy, technology and education.

The cube has 3 x 3 x 3 = 27 cells, where every cell represents the area that must be addressed in order to secure an IS. For example, an encryption-based signature can be applied to data in storage, when the three-dimensional cell of technology, integrity, and storage is being considered. This security model can be used for realizing system security via focusing on the measures needed to be taken in all 27 cells/areas.

A shortcoming of such a model (like the McCumber Cube) is that it does not provide any guidelines to instruct the practices for realizing secure ISs. In other words, one still is in need of a methodology to guide the person through the

security by design process. In Section 1.5, three directions were mentioned to approach the field of cybersecurity, namely: The individual (scientific) discipline direction (like cryptography or criminology), the system operation process direction (like in risk management) and the system development process direction. Security by design is aligned with the latter direction. In other words, i.e., security by design is concerned with a system development process. The system here is an IS, which comprises various components like software, hardware, data, people, procedures, and networks.

There are a number of phases in a System Development Life Cycle (SDLC) process. Examples of phases are investigation, analysis, logical design, physical design, implementation, and maintenance. An example of a SLDC methodology in engineering[31] is the waterfall model, where one goes through each of these phases sequentially. In every phase, the input of one phase is the output of the previous one. For implementing an IS, it may be necessary to iterate the cycle over time. For realizing secure (and privacy-protecting) ISs, further, one should consider the security (and privacy) aspects of the IS and the information it collects, uses and shares in every phase of SLDC methodology.

Like in privacy by design, in security by design one should make many trade-offs among contending values and objectives. An example of the trade-offs is: How much information must be shared with other parties who are collaboratively involved in securing a (distributed) IS so that the security of the whole is achieved while the privacy of the individual parties is not breached (see also Subsection 3.4.2 on privacy protection for security). As creating a formal model of such a complex setting is not always possible, applying conventional design methods from engineering is not always effective. We, similarly to (Araujo, Anjos & Silva, 2015), argue that design-thinking can be instrumental in such cases. Chapter 4 elaborates op adopting a design methodology based on both design-thinking and conventional design within engineering, as two complementary components, to realize the security (and privacy) by design principle systematically in complex socio-technological systems. The combined methodology can be perceived as a bridge to link the gap between the solution space and the problem space.

3.4 Interplay between privacy protection and cybersecurity

There is a close dependency between privacy protection and cybersecurity. All experts and people are aware of the fact that privacy protection requires establishing cybersecurity. Nevertheless, the other way around is not common knowledge. In this section, therefore, these inter-dependencies are elaborated upon.

---

31 Another SLDC methodology is Scrum, for more information see https://www.scrum.org/resources/what-is-scrum.

3.4.1 Cybersecurity for privacy protection

One of the pivotal principles of privacy in legal domain, see Subsection 2.3.1, is the data integrity and confidentiality principle. It specifies that data should be secured appropriately against (accidental) loss, destruction or damage as well as be kept confident against unauthorized or unlawful access and processing. Actually, the scope of this principle falls within the scope of the CIA triangular that should be protected by cybersecurity. Clearly, cybersecurity is a key necessity to protect personal information by hiding the information against unauthorized entities and/or maintaining its integrity against intentional or accidental changes.

Note that in protecting an IS against privacy risks one needs to model and consider more parameters than those considered in securing the IS. Tschantz and Wing (2009) argue that in cybersecurity you need to model a system, adversaries and the interactions between them. In privacy protection, however, one needs to model also data subjects and the contextual factors (e.g., the available background information and the social-political aspects), which evolve by definition. The extra twist in privacy protection settings mainly stems from subjectivity and extra context-dependency of privacy. The dependency of privacy protection on cybersecurity (and vice versa, as to be explained in the following subsection) is illustrated in in Figure 6.

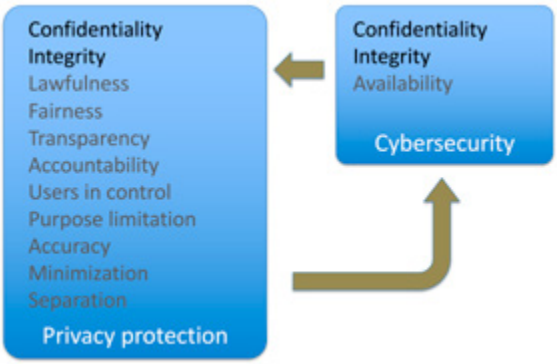


Figure 6: An illustration of the dependency between privacy protection and cybersecurity.

3.4.2 Privacy protection for cybersecurity

Dependency of cybersecurity on privacy protection (or protection of business-sensitive-data) is not a widely well-acknowledged fact. This subsection elaborates on this dependency in those cases where information sharing is necessary and/or useful for realizing effectively secure ISs. Information sharing is one of the pillars of cybersecurity, especially in distributed settings such as the Internet itself, IoT systems, and distributed Intrusion Detection Systems (IDSs). Distributed IDSs are

security-enabling systems for detecting cyberattacks. In the following, some examples of collaborative cybersecurity are provided where information sharing among various parties and/or system components is the key to realizing cybersecurity. Subsequently, two models for information sharing, i.e., a local model and a central model, are explained and the importance of privacy protection for information sharing is elaborated upon.

Examples of collaborative cybersecurity. The Internet is a typical example of a well-functioning distributed system with a huge number of stakeholders such as Internet Service Providers (ISPs), Domain Name Service (DNS) providers, and Application Service Providers (ASPs). These Internet stakeholders, in turn, are associated with a wide range of national and international institutions, public and private sectors, and academia and industries. The Internet stakeholders form a community of peers who collaborate in a participatory and bottom-up way to build up a robust ecosystem for the Internet (Internet society, 2016). Such a model of governance yields stability, integrity, and open nature for the Internet and the underlying technologies and systems. Particularly, this collaboration is crucial for maintaining the security of the Internet, as there is no central entity to monitor the Internet and enforce required security measures. This is a typical success case of collaborative security approach, which strongly relies on the underpinning *participatory* and *multi-stakeholder* principles of the Internet (Kolkman, 2017).

In the area of cybersecurity (and privacy), collaborative and cooperative solutions are used among organizations (Schafer, 2010). These solutions are already proposed and/or used for, for example, preserving user privacy (Kolter, Kernchen & Pernul, 2009), identity management (Linden et al., 2009), and intrusion detection and prevention (Zhou, Leckie & Karunasekera, 2010). Benefits of collaboration and cooperation can be at architectural, teamwork and global levels. At the architectural level it improves scalability and availability. At the teamwork level, it compensates shortcomings of individuals. At the global level, it gives the big picture, or the so-called weather report or dashboard view, which improves situation awareness about the whole system (Bye, Albayrak & Camtepe, 2010a; Bye, Camtepe & Albayrak, 2010b).

Cybersecurity incidents are usually detected by using various sensors distributed across various locations and organizations. To this end, these distributed sensors, which may belong to different organizations, share their local data in order to enable detecting those cyberattacks that aim at various targets in a stealthy way. The data collected by every sensor at a site provides a small piece of evidence about ongoing attacks (so-called, weak signals with low accuracy, certainty, etc.). Via information sharing, these sensors can join forces and the weak signals at local sensors can be combined to detect otherwise under radar cyberattacks. More

specifically, cybersecurity attacks can be detected locally or centrally by using the information collected from distributed sensors. Detecting cyberattacks locally may provide a shortsighted view on ongoing cyberattacks in case of, for example, Distributed Denial of Service attacks (DDoS attacks) whereby a large number of victims are attacked at various locations simultaneously or sequentially. Sharing information can improve awareness about such ongoing attacks.

Models of information sharing. In order to share information among a number of cooperating entities, one can use a central entity[32] that collects data from those distributed entities, enriches the data and shares the outcome with other system components (e.g., sharing the outcome with a security dashboard or with an intrusion prevention system) to somehow act upon the outcome. The shared information can be raw data as collected at local entities or enriched data processed at local entities. Therefore, the amount of data processing at local entities can vary from none-to-much (and at the central entity, the other way around). Figure 7 illustrates two sub-models of the centralized data sharing model with (a) heavily-centralized data processing and (b) lightly-centralized data processing. Figure 7 shows the amount of data processing at the central point symbolically by a large or small size of the central party, respectively. Sub-model (a) asks for sharing almost raw data and Sub-model (b) asks for sharing processed data. "Sharing raw information with a central node … may not be fruitful due to

- Creating information overload at the central point,
- Losing domain knowledge due to not communicating all the detailed contextual information to the central point, and
- Revealing business/privacy sensitive information to the central point" (Jansen, 2015).

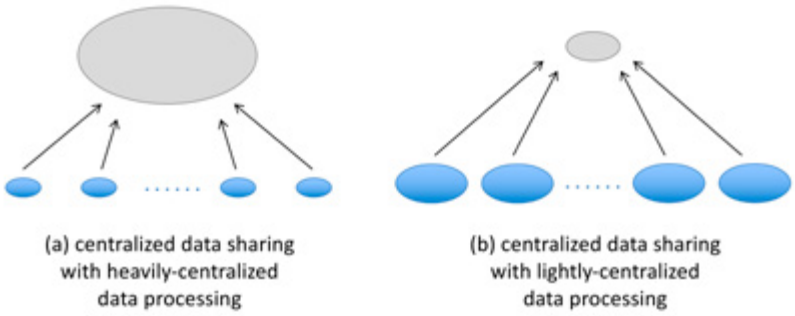


Figure 7: An illustration of the centralized data sharing models, adopted from (Cornelisse, Bargh & Choenni, 2017).

32 For simplicity, other architectural structures, like peer-to-peer and mixed models, are not considered here. Similar conclusions to those discussed here can be drawn in others models as well.

Due to the abovementioned reasons, solutions based on a heavily-centralized architecture (e.g., Security Operations Center, SOC) are inappropriate in largely distributed and cross-organizational settings. In such settings, therefore, one should find the balance between the amounts of local and central information processing. In this way, the domain knowledge can be exploited and "just relevant and aggregated information" can be communicated to the central point. At the central point, consequently, a high-fidelity view of ongoing attacks can be constructed across the whole system with a high enough accuracy and certainty (Cornelisse et al., 2017).

Importance of privacy protection for information sharing. The data collected by local entities are often privacy (and business) sensitive. Therefore, sharing such information across organizations is not self-evident as it may compromise the privacy of individuals, the competitive advantages of businesses and the national sovereignty of countries. Therefore, it is a challenge for IS designers to determine what "just relevant and aggregated information" is to share with the central node in Figure 7 so that, among others, the privacy of individuals is preserved given the purpose of data sharing in mind. For realizing ISs such as a distributed IDS, system designers should consider two types of privacy.

1. The privacy of the individuals from the local organizations that are under attack (i.e., the privacy of victims). Local organizations may not be willing to participate and share information if this information is privacy-sensitive.
2. The privacy of the individuals being suspicious as cyber attacker (i.e., the privacy of suspects). For sharing information about the possible cyberattacks it is necessary to share some personal data (like IP-addresses) of potential attackers in order to locate them effectively. As such data sharing, if done inappropriately, may lead to imposing sanctions against alleged, but not proven, cyber attackers.

Although the privacy of victims of cybersecurity attacks is evident for everybody, the privacy of alleged attackers or suspects is not well-acknowledged. The latter may cause many privacy related complications. For example, one action that can be executed based on information sharing is blacklisting, i.e., putting the alleged attacker on a list so that some sort of sanctions can be applied to the attacker. In the Netherlands blacklisting is subject to privacy legislations and is monitored by the Dutch DPA. The DPA should approve all blacklists.[33] The current legislation is very much aimed at the physical world; it should be considered how the legislation can be applied to the virtual world. For example, to blacklist someone, there should be a very strong and hard evidence against the suspect and the suspect should be informed in being blacklisted. As a distributed IDS needs to blacklist suspects and

33 See https://www.cbpweb.nl/nl/onderwerpen/zwarte-lijst.

share their information within a couple of seconds, it is unclear how and whether all the legal (and ethical) conditions for blacklisting can be met within this timeframe.

As explained above, effective cybersecurity, which asks for sharing information across organizational boundaries, requires protecting privacy and business-sensitive information. Therefore, for developing any commercially viable product, system designers should embed privacy by design principles in their security by design processes. To this end, an important design trade-off that should be made is between privacy and cybersecurity values.

3.5 Beyond just a technological approach

One of the driving forcing beyond the rising importance of privacy protection and cybersecurity is the IoT. The IoT is rapidly growing because it offers many economical and societal potentials and benefits. However, the IoT introduces also many (new) security and privacy risks.[34] The IoT is a typical ICT development that asks for realizing holistic privacy and security solutions that span beyond technological boundaries. Therefore, the case of IoT is used in this section to elaborate further on the need of adopting a holistic approach for addressing privacy and cybersecurity risks.

Harbers et al. (2018) present a conceptual framework for understanding and approaching the challenges and obstacles that arise in addressing the privacy and cybersecurity risks of the IoT. The framework identifies four fundamental challenges and presents a number of solution directions for mitigating these challenges. The framework is illustrated in Figure 8 with four challenges: IoT complexity, lack of awareness, lack of incentives, and lack of monitoring and enforcement. The two blocks on the top row show the link between privacy and cybersecurity risks (top left) and the need for adopting and developing mitigation measures (top right). Below these two components, the figure shows four IoT challenges mentioned (i.e., the blocks in orange) and the corresponding solution directions (i.e., the blocks in blue). Note that the relations between the IoT challenge blocks do not necessarily imply causality. They actually represent the most important relations surfaced in the study of Harbers et al. (2018). The nature of the complexity challenge is technological, mainly requiring solutions in the technological field. The nature of the other challenges is non-technological mainly, requiring procedural and policy-related solutions. In the following each of these obstacles are elaborated upon shortly. For detailed information and references, the interested reader is referred to Harbers et al. (2018).

34 Note that IoT devices may cause safety risks as well. These safety risks, although being relevant, are not explicitly named in this section in order to be consistent throughout the contribution.

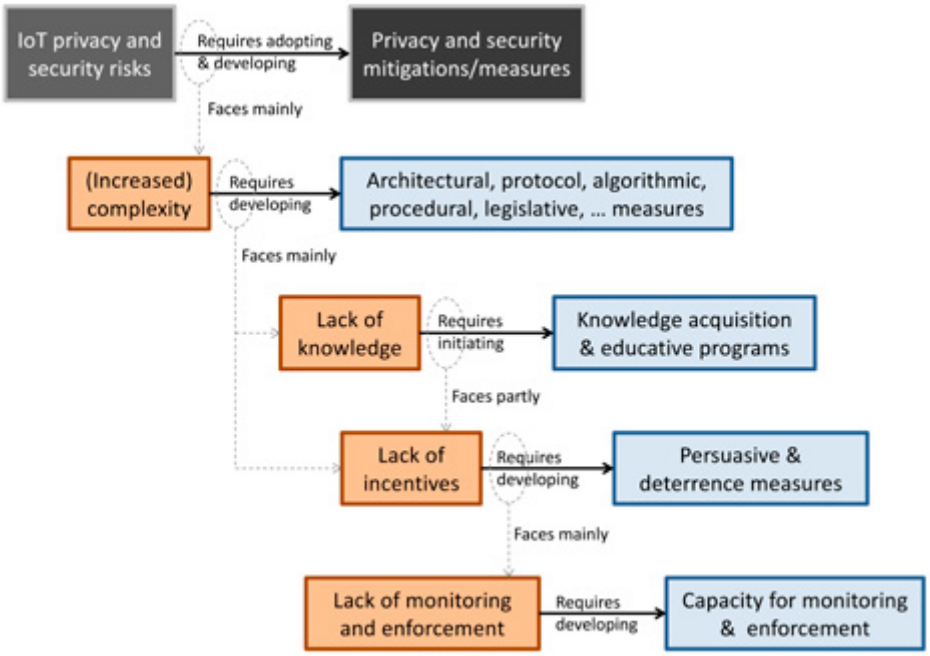


Figure 8: A conceptual framework illustrating the obstacles in addressing IoT privacy and cybersecurity risks (boxes on left side), and solution directions to overcome them (copied with adaption from Harbers et al., 2018).

IoT complexity stems from a number of factors. First, the basic architecture of IoT systems includes two layers that do not exist in traditional ICT systems. These layers are the perception layer (which includes those devices that interact with the physical world, like sensors and actuators) and the middleware layer (which includes those system components for the management and processing of sensory data and actuation signals). Second, proliferation of IoT devices creates large amounts of data of various formats, types and granularities, i.e., the big data. These (big) data can be linked to other data sets and used for different purposes, often leading to (new) personal data. Third, there is a wide range of stakeholders (e.g., citizens, scholars, entrepreneurs, and civil servants) involved in developing, deploying, and using IoT systems. Noticeably, these stakeholders are spread over various geographical, governmental, judicial and administrative boundaries, which makes it difficult to enforce appropriate rules, regulations and standards on them. Fourth, realizing efficient, scalable and interoperable privacy and security mechanisms is much more difficult for IoT than for traditional ICTs. Because, for example, malicious attackers in IoT can carry out many attack types[35], mitigation

35 So-called 'attack vectors' in the cybersecurity domain.

mechanisms devised for traditional ICT domain are inefficient for IoT domain, and many trade-offs should be made between in designing IoT systems. As such, IoT complexity is a big hurdle for securing IoT systems and protecting privacy therein. Dealing with complexity should be done at all system levels such as architectural, protocol, and algorithmic levels.

Lack of awareness and knowledge among IoT users, producers, providers, and policymakers impedes dealing with IoT complexity as shown in Figure 8. It is important to be aware of privacy and cybersecurity risks and know how to mitigate them. The human factor forms a crucial source of vulnerability in cybersecurity. As currently users lack knowledge about privacy and cybersecurity risks, they do not protect themselves adequately. Moreover, IoT producers, providers and policymakers often have insufficient knowledge about privacy and cybersecurity risks. This unawareness makes it difficult for them to develop secure and privacy-friendly IoT systems and policies. As an indication of the interplay between IoT complexity and lack of awareness, the current fast developments and high complexity of IoT systems create a lack of knowledge and awareness and the resulting knowledge gap impedes further dealing with IoT complexity, thus entering into a vicious cycle. Examples of the measures to overcome the knowledge gap are investment in education, awareness campaigns, and (scientific) research.

Lack of incentives makes it difficult to devise and apply appropriate measures against privacy and cybersecurity risks. Taking such measures often yields little benefits for the respective party. In other words, lack of appropriate incentives and motivations impedes dealing with the IoT complexity and the lack of awareness and knowledge, as illustrated in Figure 8. This lack of incentives exists for both end-users (as they don't experience the sides effects of IoT risks immediately or even ever) and companies. Small and startup companies, which are highly active in IoT market, aim at attaining first-mover advantage and often don't see any incentive for after-sell IoT product support (i.e., they see it costly to provide the after-sell product support). This is because small and startup companies expect little reputation damage if their IoT product fails. In addition to being costly, the development and implementation of privacy protection and cybersecurity measures are perceived as hinderance for the functionality, compatibility and ease of use of the product. Measures to generate incentives should mainly target companies, as end-users think that companies should sell sound products. Examples of such measure are (a) strengthening the duty of care of companies in feeling that it is their duty to take care of the whole lifecycle of their IoT products, (b) making companies accountable for the damage caused by their IoT products, and (c) creating risk insurances to cover the privacy and cybersecurity risks of the IoT. Note that currently accountability is often evaded because IoT complexity makes it difficult to pinpoint the source of the problem to take him/her accountable.

Lack of monitoring and enforcement impedes the effects of incentives. The current duty of care and accountability regulations are not specifically defined for IoT systems. This introduces uncertainties about the applicability of these generic regulations. As a result, these generic regulations on privacy and cybersecurity are limitedly monitored and enforced in ISs such as IoT. Two solution directions here are (1) to increase the capacity of supervisory authorities, and (2) to improve the current duty of care and accountability regulations by making them concrete on what an end-user can expect from an IoT system or from an IoT service provider, and within which timespan.

In conclusion, the discussion above shows that realizing an effective defense against privacy and cybersecurity risks asks for adopting a comprehensive solution package, where technological solutions play an important but not a definitive role.

3.6 Conclusion

This chapter provided an insight in cybersecurity, mainly as perceived from the viewpoint of developing secure ISs. After a brief introduction to the concept of cybersecurity and its evolution, a framework for conceptualizing cybersecurity was presented based on the critical information characteristics that are relevant for cybersecurity. The typical critical information characteristics are confidentiality, integrity and availability (i.e., the CIA characteristics).

The need for a security by design methodology is emphasized for realizing complex and distrusted ISs in a systematic way. Furthermore, it is shown that there is an interplay between privacy protection and cybersecurity. In other words, unlike most expectations, also preserving privacy is necessary for an effective cybersecurity, especially in distributed settings. This can be perceived as a gap between the situation of current practices and the desired situation.

Finally, it is shown that an effective defense against cybersecurity (and privacy) risks asks for adopting a comprehensive solution package that spans beyond just technological solutions. This can be seen as another gap between the current situation and the need for adopting a holistic approach for addressing the cybersecurity (and privacy) issues of complex and distrusted ISs.

Towards a privacy and security by design methodology

Realizing privacy-protecting and secure ISs is a challenging task (Choenni, van Dijk & Leeuw, 2010; Tschantz & Wing, 2009). This challenge exists due to a number of reasons, like uncertainty in problem definition, ambiguity of stakeholder demands, difficulty of eliciting relevant IS requirements, and the necessity of making trade-offs among many contending requirements. For example, designers should address the preferences of end-users, limitations of technologies, constraints of ethics, laws and regulations, ill intention of adversaries, societal and political values, and (unforeseen) side-effects of data analytics and ISs in operation. Moreover, some of these constraints, like the privacy preferences of data subjects, are subjective and dependent of the context (e.g., the location and time).

This chapter sketches a range of approaches for designing privacy-protecting and secure ISs in socio-technological settings. The design approaches in this chapter are discussed and presented for the case of privacy by design, rather than that of security by design. As mentioned in Section 3.4, cybersecurity is closely tied to privacy protection. Therefore, it is expected that the discussion here can be applied to security by design objectives with (minor) adaption. Further, focusing on privacy by design in this chapter adequately covers the range of the challenges that stem from subjective and context-dependent non-technological factors (e.g., ethics, privacy law, politics and sociology).

The notion of *design* is equally relevant for both engineering disciplines, which are rooted in science in its positivism sense, and in design-thinking disciplines, which are rooted in art in its constructivism sense. Design in both technological and artistic senses is the process of creating something new like a new car, a new strategic plan or a new software program (Conklin, 2005). All creative work is a process of design basically and practice-oriented problems require designing a solution through resolving the tension between what is needed (e.g., via marketing) and what can be done (e.g., via engineering). Considering this introduction, this chapter starts with describing two approaches for designing privacy-protecting ISs, one rooted in engineering disciplines (in Section 4.1) and the other rooted in design-thinking disciplines (in Section 4.2). Subsequently, in

Section 4.3 it is argued that some aspects of privacy by design asks for closely integrating design-thinking and engineering approaches.

4.1 Engineering approach

Engineering is considered as a "branch of science and technology concerned with the design, building, and use of engines, machines, and structures" (Oxford, 2019). In the cyber domain, an engineer designs, implements, deploys, and administrates an IS to address a real problem. This addressing a real problem implies that engineering coincides with applicability (Bargh et al., 2014).

Cavoukian's privacy by design principles are high-level guidelines that should be translated to actual system designs and engineering practices (Gürses, Troncoso and Diaz, 2015; Gürses & del Alamo, 2016). To carry out such a translation systematically, there is a need for a methodology. One pioneering work in the area of *privacy engineering* methodologies is proposed by Spiekermann and Cranor (2009) who present a systematic approach for guiding privacy engineers on how to design privacy-friendly ISs. Considering IS architectures at the time (i.e., in 2009), the authors identify three distinct spheres, for which engineers should devise appropriate privacy-protecting measures. These spheres are the following:

1. *User sphere*, which encompasses a user's device,
2. *Recipient sphere*, which denotes the setting in which backend infrastructure and data sharing networks are located,
3. *Joint sphere*, which encompasses those companies that host users' data and provide (often free of charge) additional services like e-mail.

For example, a WhatsApp app of a user is at the user sphere, its server is at the joint sphere, and the WhatsApp app of the user's connection is at the recipient sphere. With the advent of IoT systems nowadays, we expect that one can identify also other spheres like an intermediary sphere for collecting sensory data from the real-world, for processing these sensory data, and for providing the processed sensory data to context dependent applications and/or for executing the actuation commands issued by these applications (thus, impacting the real-world).

On the other hand, for deriving IS requirements it is necessary to have a detailed understanding of the relevant processes and the needs of the stakeholder surrounding these processes (Hoffer, George & Valacich, 2002). These needs can, in our case, be about the privacy related perceptions, expectations and concerns of system users (Cannon, 2004). Spiekermann and Cranor (2009) identify three IS tasks: data transfer, data storage, and data processing. Note that, if needed, one can extend these tasks, for example, like those typical ones of data analytics (or of AI systems), as shown in Figure 9. These tasks have different impacts on privacy, depending on, for example, where they take place (i.e., in which spheres), what kind of data (types) are concerned, and for which purposes the data are used.

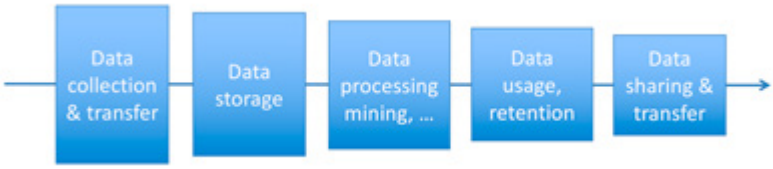


Figure 9: Tasks within a typical data analytics process (or a typical AI system).

Considering the spheres in which the data analytics tasks take place, one can interpolate the data analytics model in Figure 9 with the three spheres mentioned above to have a complete data analytics process in various spheres, as schematically shown in Figure 10. Harbers et al. (2019) call such a data processing cycle a *data journey*. Shown in Figure 10 are also the possibilities of linking the original data with other (external) data sets. Such a data linkage is a typical scenario arising in big data settings nowadays.

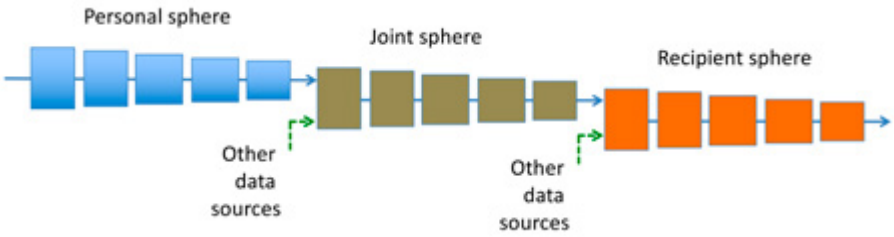


Figure 10: Data analytics tasks in three spheres, as a conceptual model to privacy risks in a data journey.

By using a data processing model like the one in Figure 10, engineers can identify privacy risks per every step of the model. This risk analysis step is similar to identifying privacy risks in Solove model shown in Figure 2. The difference with Figure 2 is that the data processing model in Figure 10 is concerned with a distributed IS (like the ISs of mobile apps or IoT systems).

In order to develop guidelines for building privacy-friendly ISs, Spiekermann and Cranor (2009) distinguish two groups of data protection measures for mitigating the identified privacy risks, namely:

1. Privacy-by-policy measures, which aim at implementing the notice and choice principles of fair information practices,
2. Privacy-by-architecture measures, which aim at implementing the minimization of personal data collection and the anonymization of client-side personal data storage and processing.

In relation to Hoepman's strategies discussed in Subsection 2.3.2, the privacy-by-policy measures encompass the inform, control and delete strategies, and the privacy-by- architecture measures encompass the minimize, aggregate and separate strategies. Note that the other strategies mentioned in Subsection 2.3.2 are not adopted by Spiekermann and Cranor (2009). Therefore, we categorize the remaining strategies of Hoepman in two complementary groups as follows:

- Privacy-by-security measures, which aim at implementing the enforce and hide strategies of Hoepman,
- Privacy-by-governance measures, which aim at implementing the demonstrate compliance strategy of Hopeman.

The extended methodology of Spiekermann and Cranor sketched so far, specifically aims at addressing the legal requirements of privacy by system by privacy engineers. Further, this methodology focuses on the boundaries between technological aspects. Although it takes into account, to some degree, the demands of data subjects (e.g., putting data subjects in control of their personal data), it does not provide a method for deriving the high-level privacy requirements stemming from ethics, social norms, specific demands of data subjects, and the needs of the end-users of the IS. In practice, there is often a gap between what users want (i.e., the actual user requirements) and how an IS is realized, due to lack of communication and cooperation between technology-oriented experts, business-oriented parties and end-users (Choenni, van Waart & de Haan, 2011a)

As argued so far, privacy by design should be addressed by integrating multiple disciplines and perspectives (like personal, legal, ethical, societal, technological and political perspectives). In the area of requirement engineering, a number of methods have emerged that integrate multiple perspectives during eliciting privacy related requirements. For example, Notario et al. (2015) argue that many sources, like end-user concerns, self-imposed policies, regulatory frameworks, prioritized risk scenarios, and best practices and standards, can be used to derive privacy requirements. The method proposed by Degeling (2016) relies on workshops and reflection-after-workshops to elucidate the privacy concerns of various stakeholders such as legal staff, business consultants, business analysts, data analysts and software architects. The method proposed by Gharib et al. (2016)

uses questionnaire and scenarios to understand "not only the requirements derived from law, but also citizens' needs with respect to privacy". Although these works aim at taking into account multiple perspectives in eliciting privacy requirements, they do not elaborate upon how the alignment and integration of multidisciplinary perspectives are carried out in practice. Further, those engineering design methods that are user-centric (i.e., engage end-users in the IS development process such as the agile software development) focus more on deriving what users want (e.g., software related functional requirements, see Vetterli et al., 2013) rather than on deriving what users really need (e.g., understanding the whole environment in which end-users are situated in order to elucidate what end-users really aspire and desire), see also (Levy, 2018).

It is not much surprising that the engineering approach for privacy by design does not focus on elucidating the high-level legal, ethical, social and personal objectives and constraints. The problems addressed in engineering are typically tamed. In the area of governance, for example, tamed policy problems are those in which the stakeholders (a) have consensus over the goals and values concerning the problems at hand and (b) are certain about the factual and cause-effect knowledge needed to solve them (Georgiadou and Recklen; 2018). Therefore, the designer (i.e., the engineer in this case) can take a lead role in designing an appropriate solution based on well-established scientific theories, guidelines and principles. Note that having consensus about the goals and values and being certain about the factual and cause-effect knowledge do not mean that solving the problem is simple. In elucidating high-level objectives and constraints, however, sometimes the stakeholders either have no consensus over the goals and values concerning the problem at hand or are uncertain about the factual and cause-effect knowledge needed to solve them. In such situations the design-thinking approach can be instrumental for addressing the problem, as will be described in Section 4.2.

4.2 Design-thinking approach

Design-thinking[36] is a methodology initially used for product and service design. Nevertheless, it has been applied to other areas where there is an interaction among people, organizations and technologies. Design-thinking has shown to be useful in settings where user needs and concerns are insufficiently formulated and are hidden in *tacit knowledge*. In such settings there are often different and poorly communicating stakeholders (Nonaka & Takeuchi, 1995). In the following, an overview of a typical design-thinking process is given (Subsection 4.2.1), some example applications of design-thinking are provided (Subsection 4.2.2), and the use of design-thinking for privacy by design is elaborated upon (Subsection 4.2.3).

36 The discussion in this section is partly based on personal communication with de Poot, Mckim & Brussee (2018).

4.2.1 Design-thinking process

The process in design-thinking, as illustrated in Figure 11, comprises the following five stages typically:

1. *Empathize,* to discover and understand the real concerns, problems, and experiences of stakeholders,
2. *Define,* to find out the deeper roots of the needs of stakeholders, particularly those of directly involved end-users,
3. *Ideate,* to explore and generate solutions for the needs identified, via formulating 'how might we' questions,
4. *Prototype,* to make prototypes (i.e., tangible objects) for (a subset of) the ideated solutions that, in the views of the collaborating stakeholders, appear to be viable.
5. *Test,* to experiment and evaluate the prototypes with the end-users and learn from them for improving the follow ups.

These stages, which may occur concurrently, are rapidly iterated and, per iteration, the prototyped artifacts (e.g., products, services, tools or processes) are tested. Practical experiences with the prototyped artifacts in every round inform the following design round about how to improve the artifacts. In the follow up iterations, the most viable concepts are worked out in greater detail to attain a viable product eventually.

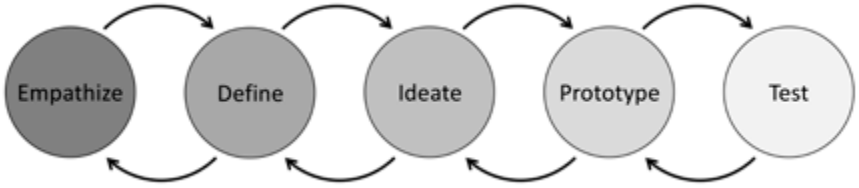


Figure 11: Stages of a typical design-thinking process.[37]

In design-thinking a good understanding of the practice field is the starting point. Further, the design process is highly collaborative – where end-users are involved in all phases to develop and improve the artifacts – and informed by practical experience. Involving end-users, especially early on in the design process, prevents disappointments in that the artifacts do not cater the real needs of users. This early involvement of end-users (or stakeholders) enables discarding suboptimal solution directions as soon as possible. This so-called *fail fast* approach gears the design process towards producing viable products with high chance of user adoption. Giving users the opportunity to give their inputs, ideas and viewpoints to the design process, is important in developing social services where citizens' participation and acceptance are of outmost importance.

37 This figure is inspired by a similar figure in http://createdu.org/design-thinking/.

4.2.2 *Applicability of design-thinking*

Design-thinking is well suited for unstructured problems, so-called wicked problems (Zimmerman, Forlizzi & Evenson, 2007). In the area of governance, for example, wicked policy problems[38] are those in which the stakeholders (1) have dissensus over the goals and values concerning the problems, and (2) are uncertain about the factual and cause-effect knowledge needed to solve them (Georgiadou and Recklen, 2018). Based on these two criteria, Table 1 presents a classification of problems to structured (or tamed) problems, unstructured (or wicked) problems, and weakly-structured problems. Using design-thinking, one can move wicked problems towards more manageable weakly-structured problems, i.e., to move upwards or leftwards from the fourth quadrant in Table 1.

Table 1: A classification of policy problems in governance (from Georgiadou and Recklen, 2018).

Problem class		Problem goals and values	
		Consensus among stakeholders	No consensus (/dissensus) among stakeholders
Special knowledge needed to address the problem	Certainty about facts and cause-effect	**(1) Tamed** or structured problems (debating on the technicalities)	**(3) Weakly structured** problems (debating goals and values)
	Uncertainty about facts and cause-effect	**(2) Weakly structured** problems (debating cause–effects and optimizing fact collection)	**(4) Wicked** or unstructured problems (endless debate)

Design-thinking aims at creating human-centric solutions that are innovative (Araujo et al., 2015), based on real end-user needs (Vetterli et al., 2013; Levy, 2018), holistic in considering the contextual circumstances (Araujo et al., 2015), and capable of having social impacts and changing mindsets (Vetterli et al., 2013; Newman et al., 2015). Design-thinking achieves these, among others, via engaging multi-disciplinary stakeholders (e.g., end-users) in the design process, via trying to emphasize with and understand users' emotions, desires, aspirations, experiences, and via allowing many failures in fast design iterations. In the area of developing ISs, design-thinking has been proposed, for example, for creating innovative mobile apps (Vetterli et al., 2013), for designing complex embedded and/or IoT systems (Araujo et al., 2015), and for devising social ISs that bring about positive social changes (Newman et al., 2015). Recently, some initiatives have suggested using design-thinking for improving the privacy protection and security of organizations. For example, design-thinking is suggested for putting risk awareness into practical

38 More formally, Rittel and Webber (1973) specify 10 properties to check whether a problem can be characterizes as wicked. This contribution does not divulge such level of details.

and collaborative action (i.e., to recruit coworkers, bosses, employees and families to work on reducing privacy and cybersecurity risks)[39] and delivering more user-focused security (i.e., building solutions that users will actually use)[40].

Design-thinking supports the process of discovering the hidden requirements of ISs, however, it faces a number of challenges when specifying these requirements. Hehn et al. (2018) mention a number of these challenges as follows:

- The coverage challenge, i.e., the design-thinking team strongly focus on user requirements, while neglecting software and system requirements,
- The traceability challenges, i.e., the design-thinking team makes weak links between needs, insights, learnings, and requirements,
- The context challenge, i.e., the design-thinking team do not formalize context requirements,
- The motivation challenge, i.e., the design-thinking team are not motivated to specify requirements systematically,
- The time challenge, i.e., the design-thinking team do not have time to specify requirements systematically, and
- The structure challenge, i.e., the design-thinking team's knowledge is implicit or captured on Post-its, while adequate tool support is missing.

It is for future research to identify and address the challenges of design-thinking when applied to the practice of protecting ISs and the personal data therein.

4.2.3 Using design-thinking for privacy by design

"Developing effective ways to tackle wicked problems is an evolving art" (Australian Public Service, 2007). The strategies that deal with wicked problems can be categorized based on how power is shared among stakeholders in the problem-solving process. According to Roberts (2000) and the Australian Public Service (2007) these categories are as follows[41]:

- *Authoritative* strategy, according to which the power of defining and solving the problem is given to a specific group or an individual, based on, for example, their knowledge (like experts) or their organizational position (like managers). The other stakeholders agree to abide by the group's or individual's decisions,
- *Competitive* strategy, according to which the power in the problem-solving process is given to all stakeholders who follow a win-lose (also called zero-sum) gaming strategy, and

---

39 See https://www.thoughtworks.com/insights/blog/design-thinking-increase-information-security-and-data-privacy.

40 See https://www.forbes.com/sites/forbestechcouncil/2018/05/22/how-design-thinking-can-change-cybersecurity/#12ee1def8d93.

41 For further detail and examples, the interested reader is referred to (Bargh et al., 2015; 2017).

- *Collaborative* strategy, according to which the power in the problem-solving process is given to all stakeholders who follow a win-win (also called non-zero-sum) gaming strategy. Via sharing the power, all stakeholders (e.g. organizations and citizens) can join forces to solve the problem at hand.

Advocates of privacy by design promote the non-zero-sum strategies in making security–privacy trade-offs (Cavoukian et al., 2012). In privacy by design cases, there are many stakeholders among whom power is dispersed and/or where the solution involves sustained behavioral changes of stakeholders. Therefore, as mentioned above, collaborative strategies, like design-thinking, should play a role in those privacy by design cases that appear to be wicked (or, at least, show aspects of wickedness). Note that design-thinking might be suitable also for purely tamed problems. However, we don't (or don't advice to) explore this track in the domain of privacy by design. This is because in such cases (i.e., the privacy problem being tamed), the laws, regulations and scientific principles to abide by are well-defined. Therefore, these rules must be followed and adhered to closely in order to implement (legal) governance measures such as accountability and liability uniformly across similar cases. In a well-functioning legal system, various objectives should be sought; the primary objective is the rule of law, where officials exercise power in accordance with the laws and regulations to achieve predictability, absence of arbitrary power to a large degree, formal equality (i.e., fairness), and order (The Hague Institute for the Internationalization of Law, 2007). For more information about this, the interested reader is referred to (Netten at al. 2018).

Using authoritative or competitive strategies might be useful in some circumstances (Australian Public Service, 2007). In some privacy by design settings, one can, to some degree, rely on also authoritative strategies where domain experts can take control of the problem-solving process due to complexity, objectivity and efficiency reasons. In this context, authoritative and collaborative strategies could be combined to harvest their benefits. For example, domain experts can actively involve some (representatives of) stakeholders in the problem-solving process, among others, to hear out their voices and standpoints, and to stimulate their commitments. Section 5.3 elaborates on this combined authoritative and collaborative strategies in the domain of privacy by design, which are coined as combined design-thinking and engineering approaches.

4.3 Combined design-thinking and engineering approach

This section elaborates on our vision for combining the strengths of a design-thinking-like approach and an engineering-like approach in order to address those privacy by design problems that demonstrate some characteristics of wickedness. Such problems arise, to the best of our knowledge, in making design trade-offs among many contending values (i.e., along multiple dimensions) (Subsection 4.3.1) and making trade-offs for actionable decisions in uncertain situations, possibly with unexpected side effects (Subsection 4.3.2).

4.3.1 Making multi-dimensional design trade-offs

Just based on legal principles, there are many trade-offs needed to be made in designing privacy-protecting (and secure) ISs, as mentioned in Section 2.4. Every design should determine which combination of the following groups of data protection measures, strategies per group, and technique per strategy should be used:

- Privacy-by-policy measures, encompassing the inform, control and delete strategies,
- Privacy-by-architecture measures, encompassing minimize, aggregate and separate strategies,
- Privacy-by-security approach measures, encompassing the enforce and hide strategies, and
- Privacy-by-governance measures, encompassing the demonstrate compliance strategy.

Based on the choices that can be made, many designs can be created. For example, for the privacy-by-policy measures, every design determines how far data subjects can be put in control of their data. This control can be at varying levels, ranging from full control to no control. Each choice, alone and in combination with other choices, has implications that should carefully be weighted and made. The EU Horizon 2020 funded project called DECODE (DEcentralised Citizen-owned Data Ecosystems), for example, focuses on developing technologies that put data subjects in control of their personal data so that they can decide how their data are shared and processed. We argue that only ensuring citizens in full control of their data, as aspired within the DECODE project, might not be the best way forward. Although putting data subjects in control of their data is necessary, it may not be sufficient to preserve privacy of individuals adequately. In analogy with an optimization problem, putting data subjects in full control of their personal data is a local optimization and does not necessarily result in a global optimization. Further, there are classical examples from the access control domain that controlling locally at end points only, can result in policy conflicts[42] and thus, in our case, lead to privacy breaches. Therefore, the design should also aim at

42 See http://www.cs.cornell.edu/courses/cs5430/2011sp/NL.accessControl.html.

investigating how to create a good balance between local control (i.e., putting data subjects in control of their personal data) and (semi-)central control (i.e., having a global intelligence that coordinates among those local polices).

Similarly, as part of the privacy-by-architecture measures, varying levels can be thought of for data minimization and aggregation in every design. In other words, every design should determine how minimization and aggregation are distributed between local and central entities. For securing data, as part of privacy-by-security approach, various technologies can be thought of, depending on the security model that stakeholders prefer to have. Example security models are: with a Trusted Third Party (TTP), with an honest but curious third party, without any third party, and with usage control or with access control. For the data privacy-by-governance measures, one can choose within a wide range of technological and procedural measures to govern the data management process according to some regulations, standards, policies and contracts as well as to demonstrate compliance to these rules and conditions.

In addition to adopting any combination of the choices mentioned above, every design can apply each of them at the various spheres of Spiekermann and Cranor (2009), using technological, procedural and/or contractual privacy protection measures. Considering all these design options together, it is evident that the design space is highly multidimensional. Thus, there might be many viable designs foreseeable for every data protection problem at hand, in a given context.

Making tradeoffs among competing values is studied, for example, by Büschel et al. (2014) between secrecy and transparency and by Fedorowicz, Gogan & Culnan (2010) between privacy and public good. These works focus only on data collection technologies or on the control of the collected data. When the number of dimensions in the design space increases, as explained above, it might be difficult to come up with some design options and choose the most viable design in a deterministic way (i.e., only by, e.g., engineers and with engineering rules). Using design-thinking, we envision, one can integrate the "true knowledge" (i.e., the models and theories from science) with "the how knowledge (e.g., the technological opportunities demonstrated by engineers) through an active process of ideating, iterating, and critiquing potential solutions to make the right thing (Zimmerman et al., 2007).

In Figure 12 the idea of creating "a series of artifacts", i.e., solutions S1, ..., S6, via design-thinking is illustrated in a simple two-dimensional design space of data disclosure risk versus data utility. This space typically arises when applying statistical disclosure control methods (Bargh et al., 2018a) as part of the privacy-by-architecture approach. Note only can design-thinking help to derive these six viable design options by making trade-offs among various criteria, it can also help the stakeholders to achieve consensus on a most viable one, for example, solution S2 shown in Figure 12.

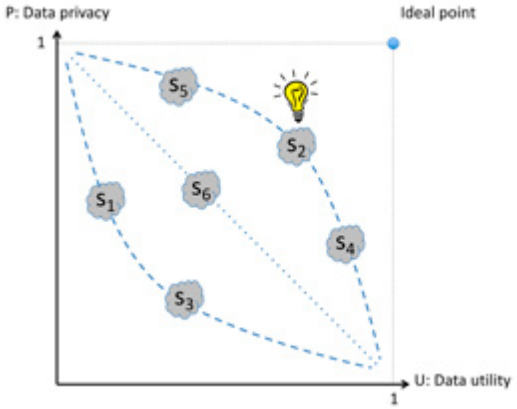


Figure 12: An illustration of creating multiple design options.

Note that under certain conditions, the contributions of such a design-thinking approach, as described above, can be recognized as research. According to Zimmerman et al. (2007), there are two ways to differentiate among design research artifacts from design practice artifacts, namely:

1. Having the research intent of producing knowledge (i.e. not just want to make a commercially viable product) and
2. Producing innovative contributions (i.e. not just refinements of existing works).

Producing innovative contributions, in turn, can be shown through describing the process, the invention, the relevance and the extensibility aspects of the executed design process (Zimmerman et al., 2007). The underlying generalizations might be formalized in the form of new theories. These, yet to be developed, theories are symbolized by the underlying dashed curves in Figure 12.

4.3.2 Making trade-offs among actionable decisions

In addition to deriving a number of viable designs and choosing the most viable design, design-thinking can be useful for fine-tuning or configuring those technological and/or non-technological data protection measures that are going to be operationalized in a complex and possibly unpredictable social context. In the following, two examples are described, one with a procedural measure and the other with a technological measure. Both these examples can be characterized as a both authoritative and collaborative strategy. On the one hand, domain experts take control over the problem-solving process due to complexity, objectivity and efficiency reasons. Combining the authoritative strategy with collaborative strategy takes place in requiring domain experts to involve (representatives of) stakeholders in the problem-solving process in order to, among others, hear out their voices and standpoints, and to stimulate their commitments.

The first example deals with creating transparency in a judicial setting through information dissemination while preserving privacy. This is shown to be a wicked problem by Bargh, Choenni & Meijer (2015; 2017a). Subsequently, Bargh et al. (2017a) propose a methodology based on design-thinking, called Transitional Action Design Research (TADR), for addressing the class of wicked problems in which privacy protection measures become operationalized in a complex and possibly unpredictable social context. Bargh et al. note:
The proposed TADR combines the Action Design Research (ADR) method with the transition management approach. The ADR method (Sein et al., 2011) considers the research process as interwoven activities of building an information technology (IT) artifact, intervening the result in an organization and concurrently evaluating it. Transition management (Kemp and Martens, 2007) is an approach that encourages reflexive governance for guiding a change process by taking small steps in strategically chosen directions.

After publishing an anonymized dataset to the public, there might be side effects due to linking the published dataset with background information and revealing personal information. Therefore, realizing a gradual change process by taking small steps in the right direction is necessary to appropriately deal with these unforeseen side effects of information dissemination. The approach of "taking small steps in the right direction" is a realization of the pre-commitment strategy[43], which is, in essence, concerned with restricting one's choices (Elster, 2000; Kurth-Nelson & Redish, 2012). Pre-commitment in the context of the first example mentioned above, can be seen as a set of restraints imposed on information dissemination policies in order to prevent potential conflicts between values such as privacy and transparency, and to enhance the trustworthiness of the information dissemination process (Meijer, Conradie & Choenni, 2014). Figure 13 illustrates such a transition management strategy that aims at achieving systemic change (Ison and Collins, 2008) through taking small steps in strategically chosen directions in the problem-understanding and solution-fine-tuning plane.

43 "For example, Cortés used such a tactic in the sixteenth century by deliberately sinking his own ships at Veracruz to compel his men to forget about retreating back" (Bargh et al., 2016).

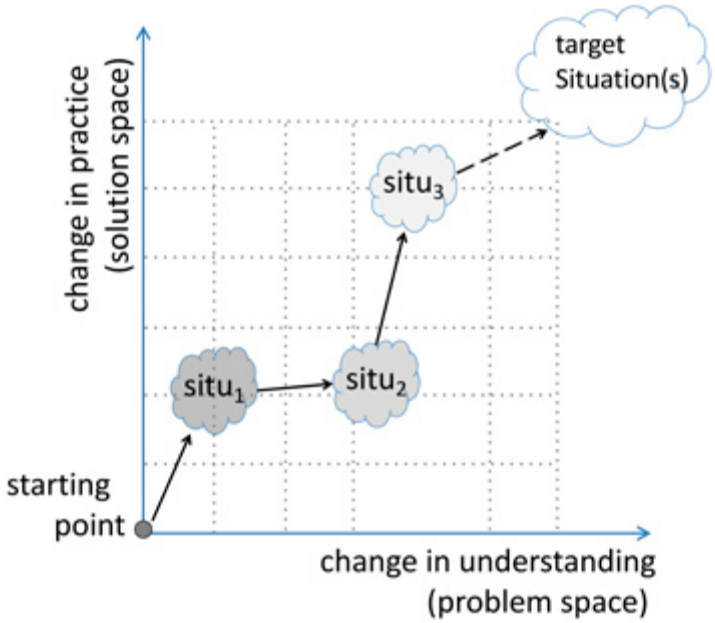


Figure 13: An illustration of the dynamics of transition changes, shown along changes in practices and in problem understandings (adopted from Bargh, Choenni & Meijer, 2017a, which in turn is adopted with adaptions from Ison and Collins, 2008).

The second example is concerned with finetuning the parameters of statistical disclosure control methods, which are technological measures to protect statistical (micro)data sets when they are shared with other parties or the public. One of these methods, whose parameter must be determined appropriately, is called the e-differential privacy (Dwork, 2006). The method is going to be used, for example, by the U.S. Census Bureau to safeguard US 2020 census data before sharing it. The value of parameter e determines the amount of the noise added to the data, thus it determines the amount of data protection and adversely the amount of data usefulness/utility. The higher e, the worse becomes privacy and the better becomes utility. In any data release context, a low value can be chosen for e and, if no side effects are observed, it can be increased gradually for future data releases, thus taking small steps in the right direction as illustrated in Figure 13.

4.4 Conclusion

This chapter sketched a range of approaches for designing privacy-protecting and secure ISs in socio-technological settings. The design approaches described are rooted in engineering, in design-thinking, and in a mix of both disciplines. The need for a systematic methodology based on a combination of design-thinking and conventional engineering design was identified necessary to bridge the gap

between the problem space (i.e., high-level requirements) and the solution space (i.e., the measures to fulfil these requirements in practice), as mentioned in the previous chapters.

This chapter presented our vision on situations where a combination of design-thinking and engineering approaches can be relevant. Such a mixed approach can be used for (a) making design trade-off among contending values in order to come up with some viable design options, (b) choosing the most viable design option among viable design options, and (c) carrying out actionable decision by making small steps in the right direction.

On positioning research at universities of applied sciences

Currently one can witness a rising volatility in various professions and expertise areas. This volatility stems from the fast pace of innovations occurring in areas such as ICT. Therefore, Universities of Applied Sciences (UASs) have aimed at embedding research skills in their curricula in an attempt to prepare their graduates for adapting to these changes (HBO-raad, 2009)[44]. In the previous chapters, some existing challenges confronting the realization of privacy protection and cybersecurity were discussed and some (practice-oriented and/or applied) research directions were outlined. In this chapter our vision[45] is depicted on the scope of the research within UASs and how the results can be embedded in the education of the UASs, particularly within ICT engineering related disciplines at the bachelor level.

This chapter starts with an elaboration of the desired research skills within the UASs (Section 5.1). Subsequently, the traditional view on applied-research and fundamental-research is described with a model, in which also practice-oriented research is projected (Section 5.2). Finally, our vision on the research at the UASs and on the way of the embodiment of the research activities in UAS education is presented in Section 5.3.

5.1 Research skills gap

The importance of acquiring and applying research skills is well recognized within the UASs in the Netherlands in recent years. Mastering research skills is seen as a necessity for UAS graduates as they will be future experts and practitioners being expected to act as knowledge-oriented professionals and innovators. In the field of

44 In Dutch: "In onze moderne samenleving is het cruciaal dat hbo-bachelors over een onderzoekend vermogen beschikken dat leidt tot reflectie, tot evidence based practice, en tot innovatie" (HBO raad, 2009).

45 Since about 2010 there have been a lot of efforts put to fill in the aforementioned gap between the actual and desired research skills. Between 2012 and 2015 we were involved in filling this gap within RUAS for computer and software engineering graduates, namely for students from Informatics (INF) education (involved in application-related software development), Media Technology (MT) education (involved in Human Computer Interaction related software development), and Technological Informatics (TI) education (involved in infrastructure related software development). The efforts resulted in developing four research courses and two publications (Bargh et al., 2014; Remijn et al., 2013). From these publications, a summary is provided in this chapter to depict our vision on the scope of the research within the UASs.

ICTs, for example, UAS graduates should translate scientific results into practice in various application domains, such as healthcare, logistics and transport, education, wellbeing and (business) administration. These professionals should be equipped with a skill set that enables them to independently consume computer science knowledge and produce useful and useable solutions for real problems in the society. In this way, these professionals will directly contribute to innovations in ICT (application) fields.

Mastering research skills for ICT graduates at the UASs has a number of advantages such as (Bargh et al, 2014):

- Not reinventing the wheel, which is achieved through investigating the-state-of-the-art works before and during devising any solution for a practical problem,
- Keeping pace and coping with fast technological advancements as witnessed in the ICT field nowadays. The skills learnt through education or experience may become obsolete in a few years. If professionals acquire no new expertise/skill during their careers, their jobs and the interests of enterprises may be put at stake,
- Learning about and adapting to the real demands and needs of customers. This ability requires having a wider view than just focusing on technological aspects (i.e., being multi-disciplinary) as nowadays ICT integrates with the fabrics of other disciplines more than ever, and
- Making innovations in fast cycles through effectively sharing knowledge with peers or colleagues and learning from others.

Previously, research was associated with theoretical studies and was out of the scope of the UASs. Therefore, there was a gap between the actual and the desired research skills for UAS students. The envisioned desired research skills for UAS students are defined along the following directions (O&K document, 2013):

- Having a researcher attitude and mentality, with which the student works methodically, interprets relevant data, reflects critically (on, for example, the objectives, assumptions, context, approach and results), forms own opinions and draws conclusions,
- Having an entrepreneurial attitude and mentality, with which the student is problem-oriented and result-driven, and tries to find practical solutions for real problems,
- Being multidisciplinary, with which the student has an eye on a broader context and reflects on the bigger picture than of own work, and
- Being communicative, with which the student conveys the solutions and the corresponding argumentations to the public and experts.

In recent years many steps have been taken in the UASs to integrate the abovementioned research skills in UAS education curricula. For framing these

research skills within the UASs, the term practice-oriented research has been coined and adopted within the UASs. In order to shed light on this term and on its difference with the traditional terms such as fundamental-research and applied-research, an analysis of these terms based on literature is carried out in the following section.

5.2 On research in general

This section elaborates on the characteristics of research, based on literature and tries to position practice-oriented research within the traditional concepts of applied-research and fundamental-research. Traditionally, research is characterized as formulated by Bargh et al. (2014).
According to Ellis and Levy (2008) research is the process of collecting and analyzing new information/data in order to enhance the body of knowledge, i.e., to create identifiable new knowledge, in an applicable domain. Similarly, Archer (1995) considers research as a systematic enquiry in order to produce communicable knowledge. In other words, research is done according to a plan (i.e., being systematic) to find answers to some questions (i.e., being inquiry based). The result of research should be understandable to an audience (i.e., being communicable) and be more than mere information (i.e., being knowledge).

When the acquired information is new for an entity (a person or an organization) but is already known in the literature of that domain, the process is not considered research (Hart, 1998). In order to determine whether an endeavor is research, one has to ask the following questions according to (Archer, 1995):

1. "Was the activity directed towards the acquisition of knowledge?"
2. "Was it systematically conducted?"
3. "Were the findings explicit?"
4. "Was the record of the activity transparent and replicable?"
5. "Were the data employed, and the outcome arrived at, validated in appropriate ways?"
6. "Were the findings knowledge rather than information?"
7. "Was the knowledge transmissible to others?"

By virtue of the definition of research, ... we believe that the term "knowledge" mentioned in question 6 is "new knowledge, in an applicable domain" (Ellis & Levy, 2008). If the answers of all these questions are yes, then the corresponding activity is considered as research (Archer, 1995).

Other than the characteristics mentioned above (i.e., being directed, systematic, transparent, replicable, and validated as well as having explicit outcomes and creating new body of knowledge), research can be specified by *generalizability* and *applicability* (Stokes, 1997). The general perception of research until the late 20th century was that research either has an application but delivers no new insight

(i.e., being applied) or delivers a new insight but has no application (i.e., being fundamental) (Offermann et al., 2009). Stokes (1997) considers this view as too simplistic and instead argues that fundamental-research is highly generalized; and that *applied-research* can create both generic and specific insights as illustrated in Figure 14.[46]

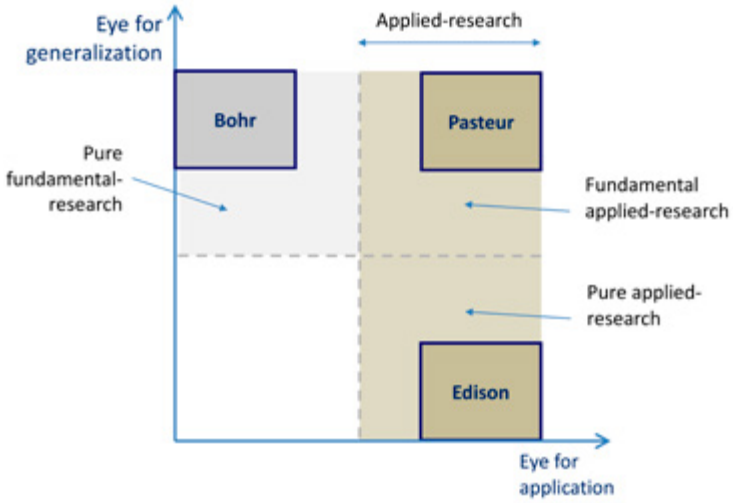


Figure 14: Pasteur quadrant, an illustration of the applied-research versus fundamental-research (based on Stokes, 1997).

The plane in Figure 14 also shows three representative examples of various research types. Fundamental applied-research is exemplified by Pasteur as a pioneer at the upper-right quadrant. The lower-right quadrant represents research-based practices, called pure applied-research, that strive for excellence and innovation through doing research to solve a real problem. This case is exemplified by Edison as a pioneer in such practices. The box with Bohr as an example of a pioneer represents fundamental-research in that quadrant.

The generalizability-applicability plane is not only relevant for research but can be applied or be relevant to the traditional practices without any research involvement, such as practices carried out by vocational professions. As an example of the case where there is no or minimum research involved, consider an ICT graduate of an UAS. After graduation the person can carry out some (routine) tasks as he/she has learnt about the corresponding skills during his/her UAS education (e.g., doing straightforward projects that require Java programming skills). In the generalizability-applicability plane such a novice graduate can be

46 Note that Stokes (1997) uses the term basic research instead of the term fundamental-research we use here.

placed at the lower right quadrant, as shown in Figure 15. Year-after-year this graduate student exercises the same java programming task in a number of similar projects and he/she acquires some experience-based tacit knowledge about his/her profession (e.g., about Java programming). This generalization is gradual and occurs in a rather slow pace. Such a gradual generalization has been a common practice in vocational endeavors throughout the years (e.g., leaning family business from parents and learning jobs skills from masters). The gained knowledge is illustrated by a dashed box in middle right side of Figure 15, assuming that the degree of generalization is medium.

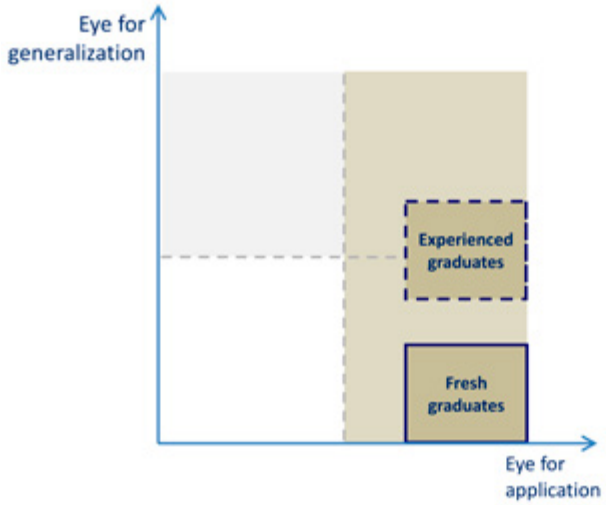


Figure 15: The generalizability-applicability plane applied to a non-research related endeavor (e.g., a vocational practice).

The situation depicted in Figure 15 symbolizes, with some level of exaggeration, the traditional situation in the UASs before the new policy of learning and mastering research skills by UAS students. In order to show the transition from the traditional situation to the current situation at the UASs, the generalizability-applicability planes in Figure 14 and Figure 15 are merged by introducing the third dimension of *research* to define a space consisting of three dimensions: *Research*, *generalizability* and *applicability* for characterizing the research within the UASs, as shown in Figure 16.

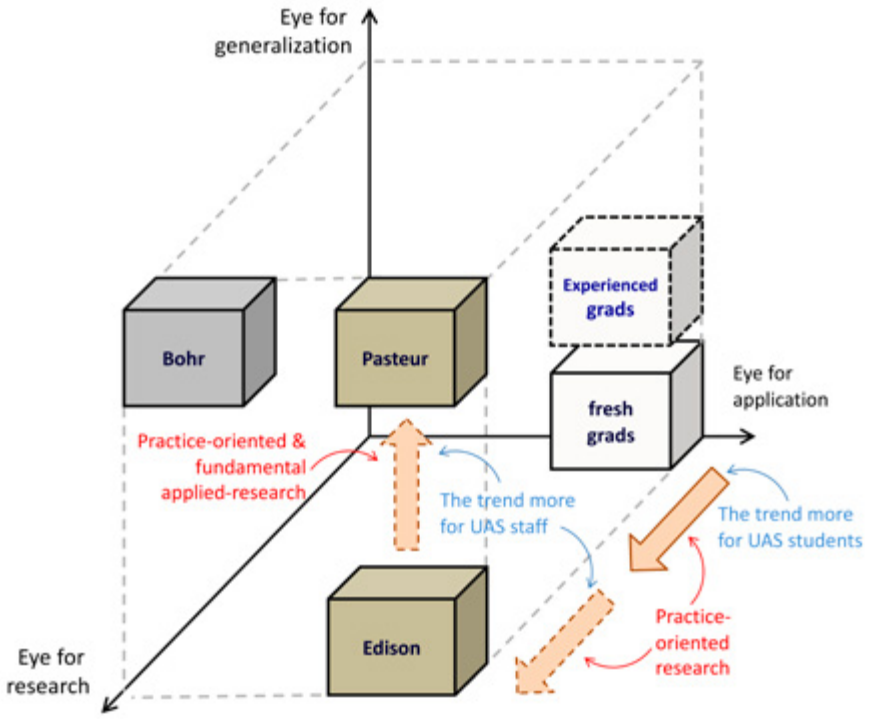


Figure 16: The 3D-model and the trend for research in UASs.

Figure 16 shows also the trends for the research within the UASs from the traditional situation to the desired situation. We distinguish two trends here: Practice-oriented research that is mainly meant more for UAS students and practice-oriented research (either in its pure applied-research form or fundamental applied-research form) that is mainly meant more for UAS educational staffs (i.e., researcher-lecturers and research chairs). These trends will be described in the following section.

5.3 A vision on research at UASs

In light of the insight presented in the previous section, one observes that the research skills sought by UASs inclines from fresh grads towards Edison, where systematic research methods are steadily applied to come up with relevant knowledge for the problem at hand. This move characterizes the practice-oriented research envisioned for UASs by experts. For example, Daan Andriessen, who is the research chair of Methodology of Practice-Oriented Research at Utrecht UAS, derives a definition for practice-oriented research from the following typical definition of research:

> *Research is a deliberate and methodical search for new knowledge in the form of answers to previously-asked questions and according to a pre-prepared plan. (Verschuren, 2009).*[47]

Andriessen leaves out or softens the terms *deliberate*, *previously asked* (i.e., in advance asked), and *according to a pre-prepared plan* and replaces the term *new knowledge* with *relevant knowledge*. In summary, Andriessen (2014) defines practice-oriented research as follows.

> *Practice-oriented research is the methodical answering of questions that leads to relevant knowledge.*[48]

The term relevant above is context dependent and for bachelor level UAS students it means being relevant for the situation and client (i.e., for the problem owner). This implies that the result of the practice-oriented knowledge is new knowledge for the client. For other contexts, like master students and PhD level researchers, the acquired knowledge should be relevant to the business sector/discipline[49] and to science and the society[50], respectively (Andriessen, 2014). In other words, the result of research becomes new knowledge for a discipline or the scientific community as one delivers more generic research outcomes.

The viewpoint mentioned above coincides with the move depicted in Figure 16 from fresh grads towards Edison, where systematic research methods are steadily applied to come up with relevant/new knowledge for the problem at hand for the client, the discipline and the scientific community. The last stop is exemplified by the Edison case, i.e., pure applied-research in terms of Stokes (1997) as shown in Figure 14. If we also move towards higher levels of generalization, as shown by an upwards arrow in Figure 16, then the practice-oriented research turns to become fundamental applied-research in terms of Stokes (1997), as shown in Figure 14.

The definition given above by Andriessen (2014) characterizes research mainly along two dimensions: Applying a systematic/valid method and creating relevant knowledge, i.e., new knowledge for the context in mind. Like Andriessen, we believe that the practice-oriented research for UAS bachelor students can aim at creating relevant knowledge for the client mainly. For other parties involved in practice-oriented research within the UASs, like researcher-lecturers and research chairs,

---

47 In Dutch: "Onderzoek is een doelbewust en methodisch zoeken naar nieuwe kennis in de vorm van antwoorden op tevoren gestelde vragen volgens een tevoren opgesteld plan".

48 In Dutch: "Onderzoek is het methodisch beantwoorden van vragen dat leidt tot relevante kennis" (Andriessen, 2014).

49 In Dutch: "vakgebied" (Andriessen, 2014).

50 In Dutch: "wetenschap en maatschappij" (Andriessen, 2014).

the bar should be set higher and one should aim at creating new knowledge for disciplines and the scientific community, given that they have (or are provided with) enough resources for doing research. This vision, which is illustrated in Figure 17, calls for researcher-lecturers and research chairs to actively publish their research results in applied-research conferences and journals.

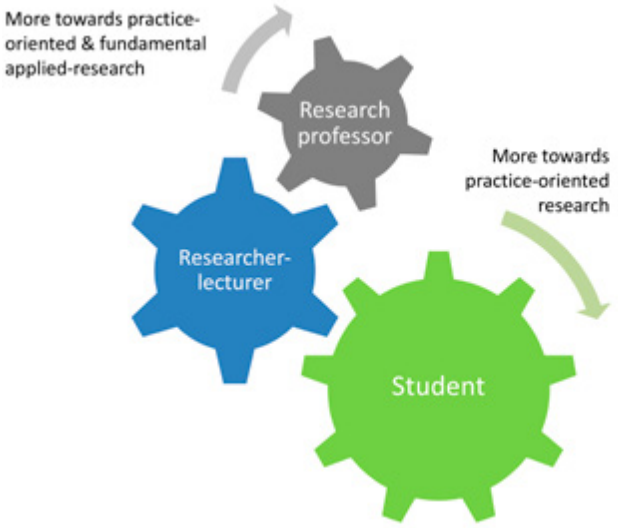


Figure 17: An envisioned model for sustainable and scalable research within the UASs.

The vision depicted in Figure 17 relies on the key role of researcher-lecturers for delivering a sustainable and high-quality research (and education) within the UASs. Being actively involved in research, researcher-lecturers can scientifically contribute to the body of knowledge and achieve higher academic degrees (interesting for master and PhD candidates) and/or be more dominantly recognized in scientific communities, industries, businesses and practices (interesting for post doctorate researchers). In addition to personal developments, the researcher-lecturers can contribute more efficiently to education by defining well-thought, practical, innovative and pioneering projects for their students and by developing new courses based on their research results. To this end, we have seen benefits of midterm and long-term research projects as a boundary object or as a platform to accommodate and nurture the research activities of researcher-lecturers within the research centers in the UASs. Therefore, a sustainable acquisition and development of practice-oriented research projects should be one of the key priorities of these research centers.

5.4 Conclusion

This chapter depicted a vision for the research within the UASs and how the research results can be embedded in education within these vocational institutions for higher education. The research in these institutions is characterized mainly along two dimensions: Applying a systematic method and creating relevant knowledge, i.e., new knowledge for the context in mind. The practice-oriented research for UAS bachelor students aims at creating relevant knowledge for the client mainly. The practice-oriented research for researcher-lecturers and research chairs, however, aims at creating new knowledge for disciplines and the scientific community, thus it is geared towards applied-research (which includes both pure and fundamental applied-research).

The researcher-lecturers at the UASs play a key role for delivering sustainable and high-quality research and embedding the research results in UAS curricula. Based on their research results, researcher-lecturers can define well-thought, practical, innovative and pioneering projects for their students and develop new courses. Moreover, research projects can serve as a platform for nurturing the research activities of researcher-lecturers at the UASs.

Reflection and future directions

ICT have created a ubiquitous digital world around people that, on the one hand, offer new capabilities and opportunities for and, on the other hand, inflict many risks upon individuals, organizations and society. Two important categories of these ICT risks are privacy and cybersecurity risks. The Research Chair on Privacy & Cybersecurity (RCP&C) at RUAS adopts a system development viewpoint to investigate *how to realize privacy-protecting and secure ISs in practice*. Accomplishing this mission will be based on performing practice-oriented and/or applied-research, while the research chair will strive to embed the research results in the educational curricula at RUAS.

This contribution elaborated upon a number of the shortcomings and challenges that exist in realizing privacy-protecting and secure ISs. In this chapter, first the main conclusions drawn in the previous chapters are summarized in Section 6.1. Subsequently, the research chair's future research plans are depicted in Section 6.2.

6.1 Main conclusions

This contribution elaborated on some shortcomings and challenges that exist in realizing privacy-protecting and secure ISs. It identified a number of existing gaps, denoting the existing distances between the current situations and the desired situations and/or between two domains that have to be coordinated in order to deliver privacy-protecting and secure ISs.

The main results in the previous chapters can be summarized as follows.

1. A wide spectrum of expertise areas is involved in the field of privacy protection and cybersecurity. Currently, the field faces a large shortage of human capital, while its market share grows rapidly (Chapter 1).
2. Privacy cannot be conceptualized in a definition with some necessary and sufficient conditions. Instead of trying to define privacy, IS designers should aim at identifying which privacy risks may arise and devise appropriate privacy protection measures accordingly. Nevertheless, in the legal domain there is a need to replace the current normative definitions of privacy by formal definitions of privacy so that these can be realized in ISs rigorously (Chapter 2).
3. Privacy protection and cybersecurity are two intertwined concepts, particularly in the context of protecting complex and distributed ISs. Not only is cybersecurity needed for protecting privacy, but also protecting privacy is necessary for effective cybersecurity in such ISs (Chapter 3).

4. Realizing privacy by design and security by design principles requires establishing a link between, on the one hand, technological and non-technological (e.g., procedural, educational and contractual) measures and, on the other hand, the high-level design requirements stemming from, e.g., legal, ethical, social, societal domains. As such, there is a need for a systematic design methodology. Design-thinking, conventional engineering, and/or a mix of these two can be adopted to systematically realize privacy-protecting and secure ISs (Chapter 4).
5. Both practice-oriented research and applied-research are relevant for UASs. Researcher-lecturers play a key role in delivering high-quality research and embedding the research results in education curricula within UASs. Based on their research, these researcher-lecturers can define well-thought, practical, innovative and pioneering projects for their students and develop new courses based on their research results (Chapter 5).

6.2 Research plans

In the (near) future, the RCP&C aims at developing an overarching methodology that integrates the capabilities of design-thinking process and engineering methods to support realization of privacy-protecting and secure ISs. Further, the RCP&C is going to study technological measures at various levels (e.g., architectural, protocol and algorithmic levels) to automate parts of the data protection and security processes and to effectively support field experts and end-users with (ICT) tools to protect ISs and the personal data therein. These technological measures, which will be developed in coordination with non-technological measures, can be devised for various stages of data analytics processes and AI-based systems, such as data collection, model extraction, and model-outcome interpretation (Choenni, Netten & Bargh, 2018). These technological measures are complimentary to non-technological measures so that data can be collected, processed and used in a fair and responsible way as foreseen in, for example, ethics as well as privacy laws and regulations.

Our main focus will be on the design and implementation of ISs according to the principles of privacy by design and security by design. More specifically, for research in the period of 2020–2023, the following research questions are posed:

1. How do we elicit the privacy and security requirements that are relevant to a certain application context?
2. How can we translate these privacy and security requirements into technological measures that are in balance with non-technological measures (e.g., procedural, contractual and educational measures)?
3. How can we make existing privacy protection and security technologies and tools scalable and user-friendly? How can we use these technologies and tools in practice?

4. How can we create an acceptable balance between the usability and privacy aspects?

For creating the balance mentioned in the last research question, putting data subjects in control of their personal data and minimizing the amount of personal information across different phases of data lifecycle (e.g., data collection, data analysis, data storage and data dissemination) will particularly be studied.

References

Andrews, E.L. (2014) Think ID Theft Is a Problem Here? Try Protecting One Billion People. Stanford Business Insights, May 1. Retrieved on May 18, 2019: https://www.gsb.stanford.edu/insights/think-id-theft-problem-here-try-protecting-one-billion-people.

Andriessen, D. (2014, October 14). Beoordelen is mensenwerk, A presentation given at RUAS,.

Araujo, R., Anjos, E. & Silva, D.R. (2015). Trends in the Use of Design Thinking for Embedded Systems. In Proceedings of the 15th International Conference on Computational Science and Its Applications.

Archer, B. (1995). The nature of research. Co-Design Journal, 2, 11.

Armerding, T (2018, October 9), Cybersecurity: Not Just "A" job - Many Jobs of the Future. Forbes website. Retrieved on May 18, 2019: https://www.forbes.com/sites/taylorarmerding/2018/10/09/cybersecurity-not-just-a-job-many-jobs-of-the-future/#2783fe9e3f2b.

Australian Public Service (2007). Tackling Wicked Problems: A Public Policy Perspective. Retrieved on May 18, 2019: https://www.apsc.gov.au/tackling-wicked-problems-public-policy-perspective.

Bargh, M.S. Meijer, R., Vink, M., Schirm, W., Braak, S. van den & Choenni, S. (2019). Opening Privacy Sensitive Microdata Sets in Light of GDPR: The Case of Opening Criminal Justice Domain Microdata. In Proceedings of the 20th Annual International Conference on Digital Government Research (dg.o), June 18-20, Dubai, UAE.

Bargh, M.S. Meijer, R. & Vink, M. (2018a). On Statistical Disclosure Control Technologies: For Enabling Personal Data Potection in Open Data Settings. Technical Report, reeks Cahier 2018-20: PU-Tools project (nr. 2889) at Research and Documentation Center WODC, The Hague, The Netherlands, 2017. Retrieved on May 18, 2019: https://www.wodc.nl/onderzoeksdatabase/2889-onderzoek-privacybescherming-methoden-technieken-en-tools.aspx.

Bargh, M.S., Vink, M. & Choenni, S. (2018b). On Using Obligations for Usage Control in Joining of Datasets. In Mori P., Furnell, S. & Camp, O. (eds.), Information Systems Security and Privacy (ICISSP 2017), Communications in Computer and Information Science (CCIS), vol. 867, pp. 173–196, 9 June, Cham: Springer.

Bargh, M.S., Choenni, S. & Meijer, R. (2017a). On Addressing Privacy in Disseminating Judicial Data: Towards a Methodology. In Transforming Government: People, Process and Policy (TGPPP) Journal, Volume 11, Issue 1, Emerald Group Publishing.

Bargh, M.S., Vink, M. & Choenni, S. (2017b). On Usage Control in Relational Database Management Systems: Obligations and Their Enforcement in Joining

Datasets. In Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP), 19-21 February, Porto, Portugal.

Bargh, M.S., Choenni, S. & Meijer, R (2016). On Design and Deployment of Two Privacy-Preserving Procedures for Judicial-Data Dissemination. in Government Information Quarterly (GIQ) Journal, Elsevier, Volume 33, Issue 3, July, pp. 481–493 (Final version published online on 28-September 2016), DOI information: 10.1016/j.giq.2016.06.002.

Bargh, M.S., Choenni, S. & Meijer, R (2015). Privacy and Information Sharing in a Judicial Setting: A Wicked Problem. In Proceedings of the 6th Annual International Conference on Digital Government Research (dg.o), May 27-30, Phoenix, Arizona, USA.

Bargh, M.S., Rooij-Peiman, A.C. van , Remijn, L.N.M. & Choenni, S. (2014). Research Skills for Software Engineering Undergraduates in Dutch Universities of Applied Sciences. In Proceedings of ACM SIGLTE, Atlanta, Georgia, USA.

Bargh, M.S., Choenni, S., Mulder, I. & Pastoor, R. (2012). Exploring a Warrior Paradigm to Design Out Cybercrime. In Proceedings of Intelligence and Security Informatics Conference (EISIC'12), pp. 84–90, August 22-24, Odense, Denmark.

Bier, C., Birnstill, P., Krempel, E., Vagts, H. & Beyerer, J. (2012). Enhancing Privacy by Design from a Developer's Perspective. In Annual Privacy Forum, pp. 73–85, October, Springer.

Büschel, I., Mehdi, R., Cammilleri, A., Marzouki, Y. & Elger, B. (2014). Protecting Human Health and Security in Digital Europe: How to Deal with the 'Privacy Paradox'? Science and Engineering Ethics, Vol. 20, No. 3, pp. 639–658.

Bye,R., Albayrak, S. & Camtepe, S.A. (2010a). Collaborative Intrusion Detection Framework: Characteristics, Adversarial Opportunities and Countermeasures. In Proceedings of International Conference on Collaborative methods for security and privacy (CollSec).

Bye, R., Camtepe S.A. & Albayrak, S. (2010b). Teams Rather Than Individuals: Collaborative Intrusion Detection. In Proceedings of Security Research Conference on Future Security, Berlin.

Cannon, J.C. (2004). Privacy: What Developers and IT Professionals Should Know. Addison-Wesley Professional.

Cavoukian, A. (2010). The 7 Foundational Principles. Retrieved on May 18, 2019: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

Crawford, K. & Schultz, J. (2014). Big Data and Due Process - Toward a Framework to Redress Predictive Privacy Harms. In 55 Boston College Law Review (BCL Rev), 93. Retrieved on May 18, 2019: http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4.

Choenni, S., Netten, N. & Bargh, M.S. (2018). On the Usability of Big (Social) Data. In Proceedings of the 11th IEEE International Conference on Social Computing and Networking (SocialCom), 11-13 December, Melbourne, Australia.

Choenni, R., Waart, P. van & Haan, G. de (2011a). Embedding Human Values into Information System Engineering Methodologies. In Proceedings of ECIME'11,

Como, Italy, 8–9 Sept.

Choenni, S., Leertouwer, E., Busker, T. & Mulder, I. (2011b). The Dark Side of Information Technology: A Survey of IT-Related Complaints from Citizens. In Proceedings of the 2nd Annual International Conference on Digital Government Research (dg.o), June 12-15, 2011, Maryland, USA.

Choenni, R., Dijk, J. van & Leeuw, F. (2010). Preserving Privacy Whilst Integrating Data: Applied to Criminal Justice. Information Policy. An International Journal of Government and Democracy in the Information Age, 15(1–2), pp. 125–138.

Conklin, J. (2005). Wicked Problems and Social Complexity. Dialogue Mapping: Building Shared Understanding of Wicked Problems, Wiley, pp. 20.

Cornelisse, R., Bargh, M.S., Choenni, R. (2016). Cybermetrics 2016: DDos en malware. A technical report by WODC, Memorandum 2017-4. Retrieved on May 18, 2019: https://www.wodc.nl/binaries/Mem2017-4_Volledige%20tekst_tcm28-286017.pdf

Degeling, M., Lentzsch, C., Nolte, A., Herrmann, T. & Loser, K.U. (2016). Privacy by Socio-Technical Design: A Collaborative Approach for Privacy Friendly System Design. In Proceedings of the 2nd IEEE International Conference on Collaboration and Internet Computing (CIC), pp. 502–505, IEEE.

Department of Homeland Security (2010, September). DHS Risk Lexicon – 2010 edition. Washington, D.C. Retrieved on May 18, 2019: at http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

Dwork, C., McSherry, F., Nissim, K. & Smith, A. (2006). Calibrating Noise to Sensitivity in Private Data Analysis. In Proceedings of Theory of Cryptography Conference, pp. 265–284. March. Berlin, Heidelberg: Springer.

Ellis, T.J. & Levy, Y. (2008). Framework of Problem-Based Research: A Guide for Novice Researchers on the Development of a Research-Worthy Problem. Information Science: The International Journal of an Emerging Trans-discipline, 11.

Elster, J. (2000). Ulysses Unbound: Studies in Rationality, Precommitment, and Constraints. Cambridge University Press.

Fedorowicz, J., Gogan, J.L. & Culnan, M.J. (2010). Barriers to Interorganizational Information Sharing in E-government: A Stakeholder Analysis. Information Society, Vol. 26 No. 5, pp. 315–329.

GDPR (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

Godkin, E.L. (1880). Libel and its Legal Remedy. Journal of Social Sciences, 12, pp. 69–80.

Georgiadou & Recklen (2018). Geo-Information Tools, Governance, and Wicked Policy Problems. In ISPRS International Journal of Geo-Information, 7, 21; doi:10.3390/ijgi7010021.

Harbers, M., Bargh, M.S., Cramer, F., Choenni, S., Nijkamp, J.E. & Nigten, A.A.M. (2019). Crafting Privacy: Two Case Studies Integrating Cross- Disciplinary

Perspectives on Privacy in Design. In Proceedings of the Workshop on Research and Practice Challenges for Engineering Interactive Systems while Integrating Multiple Stakeholders Viewpoints (EISMS19), 18 June, Valencia, Spain.

Hehn, J., Uebernickel, F., Stoeckli, E. & Brenner, W. (2018). Designing Human-Centric Information Systems: Towards an Understanding of Challenges in Specifying Requirements within Design Thinking Projects. In Multikonferenz Wirtschaftsinformatik, pp. 1051–1062.

Gharib, M., Salnitri, M., Paja, E., Giorgini, P., Mouratidis, H., Pavlidis, M. & Della Siria, A. (2016). Privacy Requirements: Findings and Lessons Learned in Developing a Privacy Platform. In Proceedings of 24th IEEE International Requirements Engineering Conference (RE), pp. 256–265.

Gürses, S. & del Alamo, J.M. (2016). Privacy Engineering: Shaping an Emerging Field of Research and Practice. In Proceedings of IEEE Security & Privacy, 14(2), pp. 40–46.

Gürses, S., Troncoso, C. & Diaz, C. (2015). Engineering Privacy by Design Reloaded, In Amsterdam Privacy Conference.

Hart, C. (1998). Doing a Literature Review: Releasing the Social Science Research Imagination. Sage Publications, the UK.

HBO-raad (2009). Kwaliteit als Opdracht, Den Haag, HBO-raad.

Hendriks, A., Brandt, D., Turk, K., Kocsis, V., In 't Veld, D. & Smits, T. (2016). Economic Opportunities for the Dutch Cyber Security Sector. Publication number: 2016-56, published by VKA.

Hoepman, J.H. (2014). Privacy Design Strategies. In Proceedings of IFIP International Information Security Conference. June, pp. 446–459. Berlin, Heidelberg: Springer.

Hoffer, J.A., George, J.F. & Valacich, J.S. (2002), Modern Systems Analysis and Design. Prentice Hall.

Internet society (2016). Internet Governance - Why the Multi-Stakeholder Approach Works, April 26. Retrieved on May 18, 2019: https://www.internetsociety.org/doc/internet-governance-why-multistakeholder-approach-works.

Ison, R. & Collins, K. (2008). Public Policy That Does the Right Thing Rather Than the Wrong Thing Righter. In Analyzing Collaborative Forms of Governance, 14 Nov, The Australia National University, Canberra, Australia. Retrieved on May 18, 2019: http://oro.open.ac.uk/27355/2/public_policy_ison.pdf.

Jansen, F. (2015, February 17). CyberDEW: A Distributed Early Warning System for Cyber Security, Technical end-report of the CyberDEW project.

Kemp, R. & Martens, P. (2007). Sustainable Development: How to Manage Something That is Subjective and Never Can Be Achieved? In Sustainability: Science, Practice, & Policy, Vol. 3 No. 2, pp. 5–14.

Kolkman, O. (2016). Trust Isn't Easy: Drawing an Agenda from Friday's DDoS Attack and the Internet of Things, weblog, October 26. Retrieved on May 18, 2019: https://www.linkedin.com/pulse/trust-isnt-easy-drawing-agenda-from-fridays-ddos-attack-olaf-kolkman?trk=hp-feed-.

Kolter, J., Kernchen, T. & Pernul, G. (2009). Collaborative Privacy - a Community-Based Privacy Infrastructure. In Proceedings of IFIP Information Security Conference Emerging Challenges for Security, Privacy and Trust (SEC), Volume 297, pp. 226–236.

Kurth-Nelson, Z. & Redish, A. (2012). Don't Let Me Do That! – Models of Pre-commitment. Front Neurosci, 6: 138. Retrieved on May 18, 2019: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3465853/.

Levy, M. (2018). Educating for Empathy in Software Engineering Course. In CEUR Workshop Proceedings.

Linden, M. , Simonsen, D., Solberg, A. , Melve, I. & Tveter, M. (2009). Kalmar Union, a Confederation of Nordic identity federations. In Proceedings of TERENA Networking Conference (TNC), Malaga, Spain.

Meijer, R., Conradie, P. & Choenni, S. (2014). Reconciling Contradictions of Open Data Regarding Transparency, Privacy, Security and Trust. Journal of Theoretical and Applied Electronic Commerce Research, Vol. 9 No. 3, pp. 32–44.

Mumford, E. (2006). The Story of Socio-Technical Design: Reflections on Its Successes, Failures and Potential. Info Systems J, Vol. 16.

Netten, N. , Bargh, M.S., Braak, S. van den, Choenni, S. & Leeuw, F. (2018). Legal Logistics: A Framework to Unify Data Centric Services for Smart and Open Justice. In International Journal of E-Planning Research (IJEPR-SI), Special Issue: Models and Strategies toward Planning and Developing Smart Cities, Ae Chun, S., Malouli, S. & Arens, Y. (eds.), Volume 7, Issue 2.

Newman, P., Ferrario, M. A., Simm, W., Forshaw, S., Friday, A. & Whittle, J. (2015). The Role of Design Thinking and Physical Prototyping in Social Software Engineering. The 37th International Conference on Software Engineering: Software Engineering in Society Track (SEIS). ACM Press.

Nissim, K. & Wood, A. (2018a). Is Privacy Privacy? In Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, Volume 376, 6 August, DOI: http://doi.org/10.1098/rsta.2017.0358

Nissim, K. , Steinke, T., Wood, A., Altman, M., Bembenek, A., Bun, M., Gaboardi, M., O'Brien, D.R. & Vadhan, S. (2018b). Differential Privacy: A Primer for a Non-technical Audience. Vanderbilt Journal of Entertainment & Technology Law.

Nissim, K., Bembenek, A., Wood, A., Bun, M., Gaboardi, M., Gasser, U., O'Brien, D.A. & Vadhan, S. (2018c). Bridging the Gap Between Computer Science and Legal Approaches to Privacy. Harvard Journal of Law & Technology 31 (2), Spring.

Nissenbaum, H. (2004). Privacy as Contextual Integrity. Washington Law Review, 79(1), 101-158.

Notario, N., Crespo, A., Martín, Y.S., Del Alamo, J.M., Le Métayer, D., Antignac, T., Kung, A., Kroener, I. & Wright, D. (2015). PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. In IEEE Security and Privacy Workshops (SPW), May, pp. 151–158, IEEE.

Occupational Outlook Handbook (2019). Information Security Analysts, April 12. Retrieved on May 18, 2019: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.

Offermann, P., Levina, O., Schönherr, M. & Bub, U. (2009). Outline of a Design Science Research Process. In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, ACM, 7.

Oxford (2019). Oxford Dictionaries. Retrieved on May 18, 2019: http://www.oxforddictionaries.com/definition/english/engineering?q=engineering.

O&K document (2013). De HR-Visie op Eindnieveau: Onderzoek pp Zijn Rotterdams (in Dutch). Ver. 1.0, February.

Petit, F. D. P., Bassett, G. W., Black, R., Buehring, W. A., Collins, M. J., Dickinson, D. C., ... & Phillips, J. A. (2013). Resilience measurement index: An indicator of critical infrastructure resilience (No. ANL/DIS-13-01). Argonne National Lab.(ANL), Argonne, IL, USA.

Poot, H. de, Mckim, M. & Brussee, R. (2018), personal communication.

Remijn, L.N.M., Bargh, M.S., Rooij Peiman, A. van & Choenni, S. (2013). A Study of Research Skills for Bachelor Students in Computer Engineering. In Proceedings of European Association for Practitioner Research on Improving Learning in Education and Professional Practice (eApril), Biel, Switzerland.

Rittel, H. & Webber, M. (1973). Dilemmas in a General Theory of Planning. In Policy Sciences, Vol. 4 (December 1969), pp. 155–169.

Roberts, N. (2000). Wicked Problems and Network Approaches to Resolution. In International Public Management Review, Vol. 1 No. 1, pp. 1–19.

Ruiter, J. de (2012), Cybercrime kost Nederland 10 miljard per jaar. Retrieved on April 10, 2019: http://www.tno.nl/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=69&item_id=2012-04-10%2011:37:10.0.

Solove, D.J. (2008). Understanding Privacy, Harvard University Press.

Schafer, J. (2010). Security Collaboration Best Practices Guide. A whitepaper by InterAction. Retrieved on May 18, 2019: https://www.eisf.eu/wp-content/uploads/2014/09/0204-Schafer-Murphy-2010-Security-collaboration.pdf.

Sein, M.K., Henfridsson, O., Purao, S., Rossi, M. & Lindgren, R. (2011). Action Design Research. MIS Quarterly, Vol. 35 No. 1, pp. 37–56.

Spiekermann, S. & Cranor, L.F. (2009). Engineering Privacy. In IEEE Transactions on software engineering, 35(1), pp. 67–82.

Star, S.L. (2010). This is Not a Boundary Object: Reflections on the Origin of a Concept. Science, Technology, & Human Values, 35, pp. 601–617.

Star, S.L. & Griesemer, J.R. (1989). Institutional Ecology, Translations and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39. Social Studies of Science, 19, pp. 387–420.

Stokes, D.E. (1997). Pasteurs Quadrant: Basic Science and Technological Innovation. Brookings Institution Press.

Pendse, G. (2018). Cybersecurity: Industry Report & Investment Case, a Report of Nasdaq Global Information Services, 25 June, Retrieved on May 18, 2019: https://business.nasdaq.com/marketinsite/2018/GIS/Cybersecurity-Industry-Report-Investment-Case.html.

The Hague Institute for the Internationalization of Law (2007). Rule of Law Inventory Report; academic part, The Hague. Retrieved on May 18, 2019: https://web.archive.org/web/20081218164026/http://www.hiil.org/uploads/File/1-947-Rule_of_Law_Inventory_Report_2007.pdf.

Tschantz, M.C. & Wing, J.M. (2009). Formal Methods for Privacy. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5850 LNCS, (August), pp. 1–15.

Verheul, E., Jacobs, B., Meijer, C., Hildebrandt, M., & Ruiter, J. de (2016). Polymorphic Encryption and Pseudonymization for Personalized Healthcare. Technical report. Retrieved on May 18, 2019: https://pdfs.semanticscholar.org/a5ec/b2f8a3b57bbfe310edabc01f435238a5c929.pdf?_ga=2.130858122.449745675.1558224204-617286979.1558224204.

Verschuren, P. (2009). De Probleemstelling voor een onderzoek. Spectrum.

Vetterli, C., Brenner, W., Uebernickel, F. & Petrie, C. (2013). Why Requirements Engineering Needs Design Thinking. IEEE Internet Computing, 17(2), pp. 91–94.

Warren, S. & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review 4, pp. 193–220.

Westin, A.F. (1968). Privacy and freedom. Washington and Lee Law Review, 25(1), 166.

Whitman, M.E. & Mattord, H.J. (2011). Principles of Information Security. Cengage Learning.

Wittgenstein, L. (2009). Philosophical Investigations. 4th edition, Translated by GEM Anscombe & PMS Hacker & J. Schulte, John Wiley & Sons.

Zimmerman, J., Forlizzi, J. & Evenson, S. (2007). Research Through Design as a Method for Interaction Design Research in HCI. In Proceedings of the SIGCHI conference on Human factors in computing systems - CHI, Vol. 7, pp. 493–502, ACM.

Zhou, C.V., Leckie, C. & Karunasekera, S. (2010). A Survey of Coordinated Attacks and Collaborative Intrusion Detection. In Computers and Security, 29 (1), pp. 124–140.

Previous releases

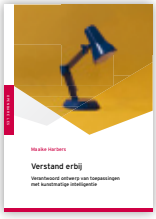
Hogeschool Rotterdam Uitgeverij

Op naar een gezonde leefomgeving. Werk maken van de wijk

Auteur	Henk Rosendal
ISBN	9789493012066
Verschijningsdatum	april 2019
Aantal pagina's	40
Prijs	€ 14,95

'Je moet op dat moment reageren en je weet nooit of je het juiste doet.' Pedagogiek in het middelbaar beroepsonderwijs

Auteur	Wouter Pols
ISBN	9789493012059
Verschijningsdatum	januari 2019
Aantal pagina's	88
Prijs	€ 14,95

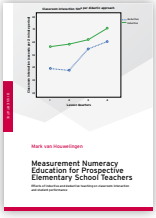


Verstand erbij

Auteur	Maaike Harbers
ISBN	9789493012035
Verschijningsdatum	november 2018
Aantal pagina's	80
Prijs	€ 14,95

Inaugural lecture

Auteur	Prof Dr Ben van Lier CMC
ISBN	9789493012028
Verschijningsdatum	oktober 2018
Aantal pagina's	80
Prijs	€ 14,95



Measurement Numeracy Education for Prospective Elementary School Teachers

Auteur	Mark van Houwelingen
ISBN	9789493012004
Verschijningsdatum	oktober 2018
Aantal pagina's	144
Prijs	€ 19,95

Schillen van het verschil

Auteur	Tina Rahimi
ISBN	9789493012011
Verschijningsdatum	juni 2018
Aantal pagina's	86
Prijs	€ 14,95

Zorg voor Communicatie

Auteur	Karin Neijenhuis
ISBN	9789051799859
Verschijningsdatum	maart 2018
Aantal pagina's	116
Prijs	€ 14,95

Next Strategy

Auteur	Arjen van Klink
ISBN	9789051799712
Verschijningsdatum	november 2017
Aantal pagina's	102
Prijs	€ 14,95

Visie op de toekomst van de Nederlandse procesindustrie

Auteur	Marit van Lieshout
ISBN	9789051799682
Verschijningsdatum	oktober 2017
Aantal pagina's	68
Prijs	€ 14,95

Slim bewegen tussen haven en stad

Auteur	Ron van Duin
ISBN	9789051799675
Verschijningsdatum	oktober 2017
Aantal pagina's	84
Prijs	€ 14,95

Techniek is belangrijk, maar het zijn mensen die het verschil maken

Auteur	Hans van den Broek
ISBN	9789051799644
Verschijningsdatum	oktober 2017
Aantal pagina's	84
Prijs	€ 14,95

Mortaza Shoae Bargh

Realizing Secure and Privacy-Protecting Information Systems:

Bridging the Gaps

9 789493 012080

Abstract

Continuous development and increasing usage of Information and Communication Technologies (ICT) introduce many opportunities for individuals, organizations and the society at large. The usage of ICT, however, increases also people's dependency on the well-functioning of Information Systems (ISs), which are, in turn, based on ICT. This dependency on ISs introduces increasing risks for individuals, organizations and the society. Privacy and cybersecurity risks constitute two important categories of such IS risks due to proliferation of personal data via ISs and the vulnerability of these systems to intentional and unintentional threats.

In order to address and contain privacy and cybersecurity risks, there is an increasing need for protecting ISs and the personal data that are collected by, stored in, and analyzed within these systems. This need shapes the mission of the Research Chair on Privacy & Cybersecurity at Rotterdam University of Applied Sciences. This mission can be formulated as: How to realize privacy-protecting and secure ISs in practice? Currently, there are gaps between the existing approaches and what is needed in practice. Bridging these gaps requires further research as well as embodiment of the research results in education curricula. As a starting point, this contribution elaborates on a number of the existing gaps and discusses some possible directions for bridging these gaps.

Mortaza S. Bargh is research professor on Privacy & Cybersecurity at the research center Creating 010, Rotterdam University of Applied Sciences. He is also part-time scientific researcher in the area of privacy and cybersecurity at the Research and Documentation Center, Ministry of Justice and Security, The Hague.

INAUGURAL LECTURE

praktijkgericht **onderzoek**

Hogeschool Rotterdam Uitgeverij

ROTTERDAM UNIVERSITY

UNIVERSITY OF APPLIED SCIENCES