



Jörg Pohle

Framing follows business models

How major private data processors frame the privacy problem

ABSTRACT

This study, conducted in 2016, analyses how four major internet-related data processing companies – Google, Facebook, Amazon, and Apple – frame privacy in their privacy policies, and how their framing of privacy is related to their particular business models. Using a security engineering approach for analysing privacy policies, the analysis is not limited to just explicit definitions and framings, but will also reveal aspects of how the companies view the privacy problem which are expressed only implicitly in the privacy policies. The analysis shows how these companies want to be seen with respect to their role as data processors – as threats to their users’ privacy, as mediators, as ‘innocent bystanders’, or even as privacy protectors –, and how these self-defined images reflect their business models.

KEYWORDS

Privacy, Document analysis, Framing, Business models, Policy documents, Technology design

AUTHOR INFO / AFFILIATION / FUNDING ETC.

Jörg Pohle is a PostDoc at the Alexander von Humboldt Institute for Internet and Society (HIIG) in Berlin, Germany, and heads the research programme “Data, actors, infrastructures: The governance of data-driven innovation and cyber security”. He also heads the project “Global Privacy Governance” that focuses on societal negotiations in the field of privacy, surveillance, IT security and data protection. Jörg Pohle studied Law, Political Science, and Computer Science at Humboldt-Universität zu Berlin, Germany. His research interests include the intersection of Informatics and Law, the research field Informatics and Society, modellification and its societal consequences, and data protection by design.

CONTENTS

0 PRELIMINARY REMARKS.....	3
1 INTRODUCTION.....	5
2 A SECURITY ENGINEERING APPROACH TO ANALYSING PRIVACY POLICIES.....	5
2.1 Adversaries.....	6
2.2 Needs, values, goals, and means.....	7
2.3 Analytical questions.....	8
3 PRIVACY NOTICES, COMMUNITY STANDARDS, AND DATA POLICIES.....	9
4 PRIVACY POLICIES IN DEPTH.....	10
4.1 Google.....	10
4.2 Facebook.....	13
4.3 Amazon.....	15
4.4 Apple.....	16
5 PRIVACY FRAMING AND BUSINESS MODELS.....	19
6 CONCLUSIONS AND FUTURE WORK.....	21
APPENDIX: LIST OF POLICY DOCUMENTS.....	23
REFERENCES.....	24

0 PRELIMINARY REMARKS

The present study was conducted in 2016 as a part of a collaborative project to shed light on the governance challenges of privacy by focusing on the processes through which privacy governance is enacted. The project was started at the closing discussion of the Berlin Early Stage Researchers Colloquium on Internet and Society in October 2014 and aimed at publishing an edited volume on “Governing Privacy – Political, Legal and Technological Developments”. The contributors convened for an authors’ workshop in June 2015 and finished all contributions in August 2016, when the edited volume was submitted to an academic publisher. In early 2017, the edited volume and its contributions failed one of two reviewers, mainly for not bowing before the Surveillance Studies’ idiosyncrasies, such as their ‘material turn’, which was influential in the very part of the Science and Technology Studies (STS) that had turned a blind eye on the technologies’ consequences for more than two decades. While this STS-internal struggle had no relevance for disciplines, such as computer science, that never lost track of the material side of the world and the technologies as well as their co-shaping of the social, it determined the negative decision of the reviewer and sealed the fate of the edited volume.

In some respects, the study is clearly outdated: firstly, all privacy policy and terms of service documents of the four companies examined here – Google, Facebook, Amazon and Apple – have been severely revised since they were last accessed in September 2016. Secondly, and even more importantly, since then two major new regulations have been enacted or entered into force: the EU General Data Protection Regulation (GDPR), which was enacted in May 2016, entered into force in May 2018, and the California Consumer Privacy Act (CCPA) was signed into law in June 2018 and became effective in January 2020. Their entry into force makes it difficult to draw conclusions because they themselves too strongly determine the structure and content of the privacy policies and terms of service documents. Thirdly, academic research has not been idle over the past six years, and a not inconsiderable number of new publications have appeared in the field of this study. Among those are studies on the framing of human rights within two of the dominant internet companies, Google and Facebook (Jørgensen, 2018), on the privacy notice-and-consent regime's openness to co-optation by corporate claimants (Cohen, 2019), on how compliance theatre (a term I use here in reference to Bruce Schneier's famous ‘security theatre’) replaces actual adherence to, and thus substantive protection by, law (Waldman, 2020), on how recent privacy and data protection regulations such as the GDPR and CCPA have led to privacy policies that are longer and harder to read and thus ‘hide’ questionable data practices (Wagner, 2022), or how companies deploy privacy, i.e. confidentiality, arguments as pretexts to keep third parties from accessing their customers' personal data (Van Loo, 2022). And fourthly, the expectation that those who process personal data would both understand that it is them and their processing which pose risks for the data subjects and admit that in their policy documents, which is captured in the remark that companies might see and present themselves ‘as threats to their users’ privacy’, has turned out to be wrong (cf. Friedewald et al., 2022: 437–438, on this blind spot in companies’ self-images). Still, it is precisely the premise on which the EU General Data Protection Regulation is built: it is the processing operations designed, implemented and carried out, i.e. controlled, by the ‘controller’ that poses risks to the fundamental rights and freedoms of data subjects (Article 1(1) and (2) GDPR); the ‘controller’ is therefore the source of those risks.

On the other hand, the results are still valid, and the method employed in this study may provide a good

starting point for further research on the relationship between business models, perceptions and framings of privacy and the design of organisational and technical means of information processing.

Still to this day, all four companies try to be seen as the guardian of their users' privacy, but they essentially do this by framing 'privacy' in a way that best fits their business interests, with their information practices virtually never representing a violation of this 'privacy'. They love to protect the 'privacy' of their users against third parties, including governments, but they remain silent at all costs of the fact that they are in an asymmetric power relationship with their users – the companies control the purposes and the means of processing personally identifiable information, including the very technologies that their users use.

The method employed in this study, i.e. reading terms of service and other policy documents from a security engineering perspective, is what makes publishing it a worthwhile endeavour, one that may be suitable for other researchers and their projects as well. From an organisational sociology-informed security engineering perspective, terms of service and other policy documents, such as privacy and data protection policies, provide a window to a company's internal conception of 'privacy'. This doesn't mean that a company's internal understanding of 'privacy' and its self-portrayal to the world are the same – they are clearly not. But they are connected and mutually shape each other. They are different, not the least because such policy documents are strongly shaped by both legal and marketing interests and language, they reflect their marketing purpose as well as their purpose of deterring supervisory authorities and competitors from suing over real or presumed violations of applicable laws. But they are also connected, firstly, as upholding a fundamental difference between the organisation's internal and external self-representations would be extremely challenging for all but the most deviant organisations. And, secondly, these policy documents are used at the same time both to communicate the organisation's values to the organisation's own employees and to educate them on what the organisation stands for and how it operates. And finally, and this is what allows for a reading of such policy documents from a security engineering perspective, among the employees that are influenced by these policy documents in their understandings of what the company stands for and how it treats users and/or customers are the systems and software developers, whose perceptions of potential uses and misuses, risks, threats as well as protection and mitigation measure are shaped by their company's self-portrayal, which in turn shapes the very technologies that these developers design and build.

Thus, analysing terms of service as well as privacy and data protection policy documents from a security engineering perspective allows for uncovering the undisclosed presuppositions – 'privacy' understandings, actors and interests as well as threat models – that underlie these policy documents, which are shaped by the company's business model or models, and which in turn shape – directly or indirectly – the design and implementation of the information processing system or systems the company uses or provides for their customers or users, which then shape, if not determine, how customers and users can make use of these systems as well as the implications for their security, privacy and data protection.

1 INTRODUCTION¹

The Snowden revelations might create the impression that the state poses the most severe threat to privacy and other related rights and interests, individual and societal alike. As this might be true with respect to the severity of the threat, the nation state is by no means the only privacy invader. Especially major internet and technology companies like Google, Facebook, Amazon, and Apple are often harshly criticised for collecting, processing, using, and disseminating information about individuals in a privacy-adverse manner.

There is already plenty of research on the relationship between privacy policies and individual privacy expectations (e. g. Earp, Antón, and Jarvinen, 2002; Earp et al., 2005; Reidenberg et al., 2015), particular legal privacy and data protection norms (e.g. Haynes, 2007; Reay, Dick, and Miller, 2009; Borghi, Ferretti, and Karapapa, 2013; Kamarinou, Millard, and Hon, 2015), or how privacy policies changed over time (e.g. Medzini, 2016 on information regulation in Facebook, almost exclusively focusing on users' privacy interests vis-à-vis third parties). On the other hand, the question of how privacy is being framed in these policies is mostly ignored by scholars (with Rizk, Gürses, and Günther, 2010 as an exception), and there is certainly a lack of research concerning the relationship between privacy policies and existing philosophical, sociological, legal and informational privacy theories. The same holds true for the question of how companies want to be seen in their privacy policies with respect to their role as data processors ('controllers' in European legal terminology) – as threats to their users' privacy, as mediators, as 'innocent bystanders', as privacy protectors etc. – and the relationship between particular framings of privacy and the companies' business models. This comes as no surprise as business models are generally covered only superficially in the literature on privacy policies (see e.g. Kuczerawy and Coudert, 2011; Rubinstein and Good, 2012).

This study analyses how four major internet-related data processing companies – Google, Facebook, Amazon, and Apple – frame privacy in their privacy policies and how their framing of privacy is related to their particular business model(s).

The rest of this study is organised as follows: Section 2 gives an introduction into security engineering fundamentals, how they can be adapted to analysing privacy policies, and which questions may guide this analysis. Section 3 will give a short overview over the four companies' policy documents which are analysed in this article. An in-depth analysis of these policies is presented in section 4. Section 5 presents an analysis of the relationship between the companies' privacy framings and parts of their business models. The article finishes with a conclusion and suggestions for addressing open issues in future work in section 6.

2 A SECURITY ENGINEERING APPROACH TO ANALYSING PRIVACY POLICIES

The main objective of security engineering is to design and develop secure information systems, which is a complex issue (Schneier, 2004; Anderson, 2008). It's well known in the IT security field what Bruce Schneier once put about claiming to have a secure product or a mechanism producing security: 'Inevitably, these claims are naïve and simplistic. ... The first questions to ask are: "Secure from whom?" and "Secure against what?"' (Schneier, 2004: 12)

¹ The text below has been prepared as of September 30, 2016.

Systems are not secure in an absolute sense but only against specific threats, attacks, and attackers. Based on conscious or unconscious design decisions, security systems may only be prepared for certain kinds of threats and attacks. The designers' experience and understanding of the context where the system is going to be deployed and operated plays a crucial role. And especially for an 'essentially contested concept' (Gallie, 1956) like privacy, the systems design is highly influenced by the understanding or ideological concept of privacy taken as a basis for design decisions.

The term 'attack' is used for two reasons: Firstly, IT security was invented by the military and inherited much of its nomenclature from the military security vocabulary. Secondly, within a system you can only observe actions and their consequences, but the system's defender – also a term inherited from military vocabulary – won't be able to differentiate between purposeful actions aimed at interfering with the system and mere usage errors. Thus, any activity that interferes with the functioning of the system is called an 'attack'. On the other hand, designers have to differentiate between real attacks and mere errors in order to design protection mechanisms which are tailored to the specifics of the respective activities.

Using a 'security' engineering approach does not mean that 'privacy' shall be seen as some kind of 'security'. Instead, it's about how to approach the design of business models, information processing, and IT systems, and the kind of questions to ask in the design process. Following Schneier, we want to ask: 'Privacy against whom?', 'Privacy against what?' and 'Privacy by which means?'

2.1 Adversaries

Attackers can be categorised into different groups: with respect to their objectives, their access to the system, their resources, their expertise, and the risk that they are willing to tolerate (Schneier, 2004: 42):

Different adversaries have different objectives: one might be the knowledge about people's preferences, habits or simply their willingness to pay higher prices for the same product or service. Public or private organisations collect and process information about people, their relationships and the society as a whole to better govern societal issues, to organise societal decision-making processes, or to find procedural solutions for substantive problems. Or they do so to better control society, to influence societal decision-making processes, or to undermine substantive rights by tweaking legal procedures.

Different adversaries have different levels of access: insiders have access to more information than an attacker from the outside. Organisations such as social network operators or service providers have access to the data which is transmitted over their networks. Law enforcement and intelligence agencies around the world have access by law on different levels. Social media systems might make it easy for its users to control the information flow by compartmentalising different groups of recipients, or make such control virtually impossible by treating everything as public by default.

Different adversaries have different levels of expertise: organisations have better expertise than individuals or groups, bigger organisations better than smaller ones. A system operator usually knows how to upgrade the system to make it easier to collect information about the system's users or to enable such collection in the first place, the users do not.

Different adversaries are willing to take different amounts of risk: corporations might more often than not

try to bend the law, find legal loopholes or exploit a law's vagueness, cases of outright violations of laws are much less likely to happen. Individuals are more averse to risking their reputation vis-à-vis their family, friends, or peers than vis-à-vis some strangers.

Reputation is an important consideration for businesses, too, because it might be hampered even if there is no proof that the company has violated the law.

2.2 Needs, values, goals, and means

There are many different privacy concepts, be it because it's 'a concept in disarray' (Solove, 2006: 477) or an 'essentially contested concept' (Gallie, 1956). Fundamentally, according to Jerry Kang privacy can be clustered into three groupings: spatial privacy, decisional privacy, and information privacy (Kang, 1998). This article will focus on information privacy only. Some scholars see privacy just as another word for secrecy (e. g. Schneier, 2004), some equate privacy with confidentiality (e. g. Ware, 1967). Alan Westin's definition of privacy refers to the individual's, group's or organisation's control of the dissemination of information about them (Westin, 1967), a definition widely shared in academia and the general public alike but by no means hegemonic. Paul Müller framed privacy as the integrity of the social role-playing (Müller, 1975), Bernhard Hoffmann defined the goal as 'preserving the original context' (Hoffmann, 1991: 127), while Helen Nissenbaum conceptualised privacy in a similar vein as 'contextual integrity' (Nissenbaum, 2004). Ruth Gavison argued that privacy should be seen as accessibility to the individual (Gavison, 1980), while others argue for privacy as a matter of fairness in the processing of personal information (e. g. U.S. Department of Health, Education, and Welfare, 1973; Rotenberg, 2001) or due process (e. g. Vries, 2013). And Spiros Simitis argued that the problem is created by automated processing generating categorisations which are then used to label individuals to be treated 'as a member of a group, the peculiar features of which are assumed to constitute her personal characteristics' (Simitis, 1987: 719; cited by Gandy, 1993 who termed it 'panoptic sort').

But there are not only concepts of privacy competing for the most convincing explanation of modern day's information practices' consequences for individuals, groups, organisations and the society. After the early German discussion about the privacy problem threw the term 'privacy' as well as the so-called 'public/private divide' into the dustbin of history (Pohle, 2016), Adalbert Podlech defined 'Datenschutz' as 'setting and enforcing the conditions under which the information practices of a given society may be acceptable for all parts of that society' (Podlech, 1976: 313). Surveillance studies scholars, too, focus on analysing real-world information practices, sometimes with and sometimes without taking any assumptions about privacy as the subject of protection (e. g. Lyon, 2003; Marx, 2015).

There are differences with respect to the means for protecting privacy, too: access control mechanisms (e. g. Hung, 2005) or information flow control measures (e.g. Ortmann, Langendörfer, and Maaser, 2007), allocating rights like access to data subjects or imposing duties like purpose-binding onto data processors (for a well-designed combination of both approaches see Steinmüller et al., 1971), educational programs and privacy icons or labels (e. g. Hansen, 2009; Kelley et al., 2009) or protection goal-based operationalisation (e. g. Hansen, Jensen, and Rost, 2015). Many scholars treat anonymity as a means for achieving privacy (e. g. Rossum et al., 1995), some as a broken means (e. g. Ohm, 2010), while others treat them as disparate concepts (e. g. Shmatikov, 2011).

Obviously, different concepts and theories claim different needs, values, or protection goals as their defining elements. And apparently, at least some system requirements depend on the designers' choices for or against a particular theory. Unfortunately, none of the companies' privacy policies or other official documents analysed in this paper include references to a particular privacy theory serving as a basis for the specific rules they contain. Despite the fact that the described theories differ on many levels, they all refer to or imply a set of rules for handling information about individuals. Therefore, to analyse how the privacy problem, i.e. how 'privacy' is understood and which activity is considered an issue for this 'privacy', is being framed by data processors one can look at their statements concerning the rules for information handling they declare to be bound to.

Privacy policies are a valid substitute for analysing how data processors are tackling the privacy problem within their products and services, and how they are trying to solve it. First of all, companies use them to communicate to their customers and the general public which standards they want to adhere to while collecting, storing, processing, using, and disseminating information. Secondly, these policy documents are prevalently binding the companies to their commitments by law (see e. g. Livingston, 2011). And commitments they are: at least one of the four companies analysed is declaring explicitly that their published 'Privacy Principles help guide decisions we make at every level of our company.' There is no hint whatsoever that this would not include systems' design decisions.

2.3 Analytical questions

The first question to ask is: 'Which players are mentioned in the privacy policies?' The company and the data subject, the latter often called 'user' or 'customer', are the obvious stakeholders. But usually there are more players on the ground, e. g. other individual users on a platform or a social network, companies with their own representation on the platform, businesses processing information on behalf of the company which owns and runs the platform, or different third parties.

Next, one has to ask which information-related interests and actions are attributed to which players. Stakeholders' interests mentioned in a privacy policy might include goals pursued by them, or purposes for which they want to collect, process and use personal information. While many of these may be widely seen as legitimate, privacy policies might also refer to criminal or socially unacceptable interests like stalking, identity theft or spamming.

Some of the information-related actions mentioned in these policy documents are generally attributed to organisations, such as collecting, storing, deleting, disseminating, publishing, processing – merging, linking, computing –, analysing, and using information. Other actions are generally attributed to users: passing information to others, entering data on websites, sending messages, publishing personal information or other content, surfing the web etc. Privacy policies might also refer to actions generally considered malicious like snooping, stealing information, or breaking into a user account. Furthermore, there are typical follow-up actions to preceding information processes like showing ads, contacting users or selling information.

This leads to the next question: 'Which interests and actions are explicitly or implicitly described as threats to the user's privacy?' A complementary question helpful for uncovering the framing of the privacy issue would be: 'Which actions are mentioned as supporting the protection of the user's privacy?' One regularly

seen statement in this direction reads as follows: ‘We use strong encryption to protect the privacy of your data’ – unfortunately without shedding light on the relationship between ‘privacy of individuals’ and ‘privacy of data’.

Finally, based on a comparison between the privacy policies of Google, Facebook, Amazon, and Apple in framing the privacy problem, it is possible to analyse how the framing of privacy in the privacy policy is related to each company’s business models as they are pursued by collecting, processing, using, and disseminating information.

3 PRIVACY NOTICES, COMMUNITY STANDARDS, AND DATA POLICIES

The following section will give a short overview over the four companies’ policy documents analysed in this article. All documents were last accessed September 30, 2016.

Google’s ‘Terms of Service’ (see Appendix, p. 18, for a comprehensive list of the policy documents analysed) are not exhaustive, ‘sometimes additional terms or product requirements (including age requirements) may apply’. The same holds true for the ‘Google Privacy Policy’, which is supplemented by a document explaining privacy and information processing–related terms Google’s users might be unfamiliar with, simply called ‘Key terms’. The company also has a webpage called ‘Technologies and Principles’ which is not incorporated in its privacy policy while at the same time propagating that the principles therein ‘help guide decisions we make at every level of our company’. Additionally, some of the questions in Google’s ‘FAQ’ and its associated answers relate to privacy issues as well. Last but not least Google has published a landing page bearing the title ‘Explore easy-to-use safety tools’ with short explanatory information about tools for users to manage personal information, control its collection, and sometimes its dissemination.

Facebook’s terms of service are called ‘Statement of Rights and Responsibilities’. The company has published a page with the title ‘Privacy Basics’, but it relates only to the relationship between a user and other users as well as third parties on Facebook, a topic further explicated on Facebook’s ‘Community Standards’ page. Facebook’s own information practices are governed by its ‘Data Policy’. Like Google, Facebook supplements its policy documents by an explanatory page in the company’s help centre, ‘Cookies, Pixels & Similar Technologies’.

Amazon’s most important policy document is its ‘Conditions of Use’ specifying the conditions under which the company provides its services. The company’s information practices are published in the ‘Amazon.com Privacy Notice’. There is only one other privacy-related policy document, addressing ‘Interest-Based Ads’.

Apple has published three relevant policy documents: the ‘Apple Website Terms of Use’, the ‘iCloud Terms and Conditions’, and the ‘Apple Media Services Terms and Conditions’. Apple’s ‘Privacy Policy’ applies generally to all its products and services. Like Google, Apple presents the user with additional policy documents, but in this case depending on the user’s location, like a document referring to ‘California Privacy Disclosures’ and ‘Information Regarding Commercial Electronic Messages in Canada’ for its Californian and Canadian users. Additionally, Apple has published ‘a message from Tim Cook about Apple’s commitment to your privacy’. The message is right on Apple’s central privacy page

www.apple.com/privacy/, leading to another three privacy-related documents: the 'Our Approach to Privacy' page about 'powerful safeguards [built] into our operating systems, our apps, and the devices themselves', the 'Manage Your Privacy' page with 'information about powerful features that help you make your devices and data secure, along with tips for avoiding fishing scams and keeping your account safe', and the 'Government Information Requests' page.

4 PRIVACY POLICIES IN DEPTH

4.1 Google

While the Privacy Policy (PP) is the most relevant document governing Google's handling of personal information, the Terms of Services (ToS) also contain specific rules concerning this issue:

'Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.'

In its ToS, Google has also included a statement on the dissemination of personal information to make user interactions, such as +1's, reviews and comments, visible to others, 'including displaying in ads and other commercial contexts', and states that it 'will respect the choices you make to limit sharing or visibility settings in your Google Account'.

In the PP's first section – 'information we collect' –, Google explains what information it collects in which ways, either directly, i. e. information the user gives Google, or indirectly, i. e. information Google gets by watching the users' interactions with its services (server-side logging) and by information transmitted by the users' devices (different kinds of device identifiers – hardware and software –, sensor data, cookies etc.), all of which are associated with the user's Google account. At least twice Google also refers to the purpose of its information collection. In the section's introduction, it's described in a very broad manner: 'We collect information to provide better services to all of our users [...]'. Subsequently, this is rendered more precisely by referring to Google Analytics which 'helps businesses and site owners analyze the traffic to their websites and apps'. The second section – 'how we use information we collect' – then is all about the purposes: 'to offer you tailored content', 'giving you more relevant search results and ads', 'to improve your user experience', 'to have our services appear in the language you prefer', and 'to make it easier to share things with people you know'. Google restricts itself in only two areas. First, the company declares to respect the user's choices 'to limit sharing or visibility' while disseminating personal information. And second, Google asserts that 'when showing you tailored ads, we will not associate an identifier from cookies or similar technologies with sensitive categories, such as those based on race, religion, sexual orientation or health'. On the other hand, the PP contains a qualified exemption clause: 'We will ask for your consent before using information for a purpose other than those that are set out in this Privacy Policy.'

This exemption clause is rather surprising, as many purposes explicated in the PP are either extremely broad and abstract, or just used as examples for broad and abstract purposes. Besides an outright sale of personal information (which Google does not, contrary to popular allegation, and explicitly denies), every other information use seems to be included in either the 'to provide, maintain, protect and improve [services], to develop new ones, and to protect Google and our users' or the 'to offer you tailored content' clause. Within

the first two sections of its PP, Google explicitly mentions the term ‘privacy’ only thrice (not counting ‘privacy policy’ or ‘privacy policies’): for stating that ‘your privacy matters to Google’, for referring to the ‘controls to manage your information and protect your privacy’, and in defining the purpose of its Privacy Policy to make clear ‘how we’re using information and the ways in which you can protect your privacy’. For Google, privacy therefore seems to be something not primarily related to Google itself and its information practices, but solely to the user.

The term ‘privacy’ is then mentioned again, when the user first gets to have a meaningful choice concerning Google’s use (and partially its collection) of personal information: ‘People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used.’ While the user is allowed to control the collection of information in cases like search queries or YouTube videos watched, concerning Google’s advertising the user may only opt-out the possible use of information, but not the collection itself. Three of seven items related to the user’s ‘choices’ are referring only to what will be shared with other users or the public.

The PP mentions four conditions under which Google shares personal information with companies, organisations or individuals outside of Google: the user’s consent, with domain administrators if the user’s Google account is managed by a domain administrator, for external processing, and for legal reasons, while Google may share information that the company itself deems to be ‘non-personally identifiable’ with everyone. Near the end of the PP’s section on sharing, Google explicitly calls its own duty with respect to this sharing ‘confidentiality’. The same understanding underlies Google’s remark that it expects external processors complying ‘with our Privacy Policy and any other appropriate confidentiality and security measures’.

The remainder of Google’s Privacy Policy is about information security, i. e. ‘to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold’, about when this PP applies, about compliance and cooperation with regulatory authorities, about changes of said policy, and contains links to other ‘useful privacy and security related materials’.

The PP is supplemented by a document explaining privacy and information processing-related terms Google’s users might be unfamiliar with, such as ‘personal information’, ‘non-personally identifiable information’, ‘sensitive personal information’, and ‘sensitive advertising categories’. Google defines ‘personal information’ as information ‘which personally identifies you [...], or other data which can be reasonably linked to such information by Google’, while information ‘about users’ is non-personally identifiable if it is recorded ‘so that it no longer reflects or references an individually identifiable user’. Only in some few cases, Google explicates in the ‘Key terms’ which kinds of information it deems to be personally identifiable. The fact of information being personally identifiable is somewhat concealed from the user by Google differentiating between the identifiability of individuals and of the users’ browsers or devices.

On its ‘Technologies and Principles’ page, Google states that ‘we work hard to make sure any innovation is balanced with the appropriate level of privacy and security for our users’, and ‘Our Privacy Principles help guide decisions we make at every level of our company, so we can help protect and empower our users while we fulfil our ongoing mission to organize the world’s information.’ Both statements pick up the ‘balancing privacy with something else’ argument widely found in privacy debates, where privacy is never

to be seen as something absolute or as an unconditional requirement.

In a quite similar vein, Google formulates its first principle as ‘use information to provide our users with valuable products and services.’ To begin with, in this paragraph Google admits indirectly that it collects information first, and then tries designing a system around this information collected. Furthermore, while Google refers explicitly to users sharing information with the company, the company omits that it also collects and uses information obtained by monitoring user behaviour and user interactions on their sites and with their products. The same applies to the third principle ‘make the collection of personal information transparent’ which also only refers to information explicitly shared with Google like comments in Blogger blogs or uploaded photos, but keeps quiet about all information which Google obtained by monitoring user interactions.

Google’s second privacy principle seemingly aims at developing ‘products that reflect strong privacy standards and practices’, but is directed at helping ‘users manage their personal information’ only. The ‘strong privacy standards and practices’ Google is referring to here are only those within the confines of what enables Google to process and use as much information as possible – no surprise then that they are not directed at data minimisation. Even the mechanisms for compartmentalising information are for addressing third parties only, like in the case of ‘circles’ in Google+ to protect the integrity of the user’s social role-playing.

The fourth principle, ‘give users meaningful choices to protect their privacy’, seems to implicitly include choices ‘over the use of their personal information’. Actually, this choice does not prevent Google from scanning personal emails, which the users cannot even opt-out of. The ‘privacy tools’ Google is referring to in the text specifying this principle are more often than not security, but not privacy tools, like ‘encrypt the search traffic between your computer and Google’. Or they are at least highly ambiguous, as the ‘browse the internet in private’ promise, because Google on the other hand warns – incidentally in its own Privacy Policy – that for example by disabling cookies ‘many of our services *may not function properly*’ (original emphasis).

According to Google’s fifth privacy principle, the company wants to ‘be a responsible steward of the information we hold’. This principle, too, only refers to security issues: the responsibility Google is talking about only applies to ‘protect the data that users entrust to us’. Therefore, it comes as no surprise that Google states that it takes ‘security issues seriously [...] to make the Internet safer and more secure.’ Google thus uses its commitment to security as a justification for using automated scanners, i. e. on users’ emails.

In its PP as well as in its Privacy Principles, Google is referring to their ‘Explore easy-to-use safety tools’ page, where it introduces different tools to their users with a short accompanying text. Unfortunately, none of the Google ‘tools’ presented under the heading ‘Be Secure’ and a mere third of those under ‘Your Privacy’ refer to privacy interests against Google. This includes the possibility to manage at least parts of the information stored by Google about its users, e. g. ‘Review your account history’. It is not clear that this ‘tool’ really is for managing privacy in a comprehensive sense: Google employs cross-site requests if one clicks on a search result link. This means that the browser does not send the HTTP request directly to the site which the user requested by her click, but to Google (and its servers) to be then forwarded to the target site, enabling Google to learn (and store and use) every click users make on a Google search result link.

Google does not make it transparent if deleting entries in ‘your account history’ refers to these traces or not. Additionally, ‘Your account, your data. Download a copy’ might refer to privacy vis-à-vis Google, depending on what ‘personal information’ one can download from Google. If this ‘tool’ refers to documents, photos and other information or data owned by the user, it addresses not privacy, but property interests. Finally, ‘Control your browser privacy’ clarifies that Google’s services and products are surveillance-by-default: ‘When you turn a privacy setting off, that information will not be sent to Google.’

4.2 Facebook

Facebook’s ‘Statement of Rights and Responsibilities’ is the company’s terms of service (ToS) that governs the relationship between Facebook and its users. Additionally, it governs Facebook’s relationship with non-users if they are surfing a website which uses Facebook’s services like the company’s share button. Like Google’s ToS, Facebook’s ToS explicitly refer to the company’s ‘Data Policy’ for information about ‘how we collect and can use your content and information’ but also contain such rules. Privacy is the first issue Facebook addresses in its ToS, opening with: ‘Your privacy is very important to us’, followed by ‘how you can use Facebook to share with others’. Facebook’s own information practices come second.

On the one hand, the ToS cover many aspects of Facebook’s information practices in depth that one might rather expect to see covered in the ‘Data Policy’. An example is Facebook’s clause ‘About Advertisements and Other Commercial Content Served or Enhanced by Facebook’. Using Facebook, users give their permission to use every imaginable piece of information or data related to users and non-users alike such as the ‘name, profile picture, content, and information’ ‘in connection with commercial, sponsored, or related content’. On the other hand, practices clearly as important as this one – like the collection and use of information obtained by monitoring ‘actions taken by users’ – are only superficially addressed in the ToS, formulated in an overly broad manner, without any detailing explanations, and simply referring to the ‘Data Policy’:

‘By using or accessing Facebook Services, you agree that we can collect and use such content and information in accordance with the Data Policy as amended from time to time.’ (all emphasis in original)

Like Google’s PP, Facebook’s Data Policy begins by listing what kinds of information the company collects, followed by a list of purposes the information is to be used for.

Facebook uses ‘all of the information we have’ to ‘provide, improve and develop services’, personalise content, and make suggestions. This includes any information created by users. In addition, all of this information is used for marketing communications by Facebook as well as for showing third-party ads and measuring their effectiveness and reach. Following a major public uproar (see e. g. Guynn, 2014), Facebook has since appended its list by stating that the company uses information for research purposes as well. Facebook also states that it will use all information to ‘promote safety and security’, ‘such as by investigating suspicious activity’, and working hard ‘to protect your account’. Besides other rather superficial information like ‘automated systems, and advanced technology such as encryption and machine learning’, the Data Policy provides just a glimpse into the means employed for Facebook’s information practices in that ‘cookies and similar technologies’ are used.

The dissemination of information – uniformly called ‘sharing’ by Facebook – takes up a big part of the Data Policy, basically divided in two sections: ‘Sharing On Our Services’ and ‘Sharing With Third-Party Partners and Customers’, supplemented by a third section, distinctly separated from the first two: ‘How we respond to legal requests or prevent harm?’ On Facebook, sharing is widespread – as one would expect on a social networking service. But by using the same term for two fundamentally different kinds of information flows – between users on the platform (i. e., mostly between equals, basically bidirectional information flows), and from users (and non-users) to third parties (i. e., an imbalanced power relationship, basically unidirectional information flows) – Facebook not only levels this difference, but hides the different consequences, too.

While Facebook allows its users to select their audience with a mechanism, resembling Google+ Circles, which protects the integrity of the social role-playing – or to share information ‘with a public audience’ –, the policy does not say anything about possible uses or restrictions. According to the section about ‘people that see content others share about you’, the company is outsourcing the task of solving interpersonal privacy issues with ‘social reporting’. This makes sense if there is no structural power imbalance between the actors involved, and therefore privacy can be negotiated in a meaningful sense. It is however unclear what would happen if there is power asymmetry, as usually between a company and an individual (Pohle, 2015). In this case, Facebook would second-order privatise rule enforcement, while the company itself created the risk in the first place. The same holds true for ‘apps, websites and third-party integrations on or using our Services’. Facebook creates a privacy-risky environment enabling others to infringe on the privacy of individuals, while absolving itself from any liability.

Facebook also ‘shares’ all information ‘within the family of companies that are part of Facebook’, therefore integrating personal information into comprehensive profiles across platforms, contexts, and roles. With respect to ‘advertising, measurement and analytics services’, Facebook states that it will not share personal information with partners in these areas ‘unless you give us permission’.

Facebook’s definition of personal information is certainly one of the narrowest in the industry, defining personally identifiable information as ‘information like name or email address that can by itself be used to contact you or identifies who you are’. This definition ignores all debates about information integration and linkage, and the possibility of identifying individuals or applying decisions onto them (e. g. Hoffman and Miller, 1973; Sweeney, 2002; Hansen, 2008; Ohm, 2010).

From ‘vendors, service providers and other partners’ Facebook only demands adherence ‘to strict confidentiality obligations’, clearly identifying the concept of privacy applied by Facebook.

Concerning intervenability options, Facebook also presents the user with little choices: users may manage only ‘the content and information you share’, but not information obtained by monitoring user actions. Information is retained by Facebook as long as possible; the necessity principle Facebook seems to adhere to in its Data Policy is loosened significantly by its application to any and every product and service Facebook provides, not only current ones, and not only the ones specified in the Data Policy (‘including those described above’).

While Facebook called its privacy policy ‘Data Policy’, the company has also published a webpage referred to as ‘Privacy Basics’. The major difference is that the former extensively addresses the informational

relationship between Facebook and its users as well as non-users, while the latter solely refers to relationships of users and non-users among each other. For Facebook, privacy seems to be an issue only among its users. The subheadings in the 'Privacy Basics' only refer to the users' relationships with others: 'What Others See About You', 'How Others Interact With You', 'What You See', and 'How to Keep Your Account Secure'.

In 'control over who sees what you share on Facebook', almost none of the choices are about controlling the collection and use of information by Facebook. Even deleting a user's Facebook account is problematic since 1) Facebook does not state that it will delete anything on their systems if the user deletes her account, and 2) if you click on 'Account Deactivation and Deletion' and skip the information about account deactivation, Facebook refers the user to consult the 'Facebook Help Center'. Facebook might delete every information about the user within 90 days, but this assumption may also be erroneous since Facebook states that 'it may take up to 90 days to delete all of the things you've posted'.

Users also can 'learn about features to help protect your account and things you should avoid'. In this section one learns what Facebook does 'to help keep my info secure'. Besides 'top-rate security measures', 'secure browsing' and 'tools to detect if you have viruses on your computer', Facebook states in this (security) section that 'when it comes to your personal information, we don't share it without your permission (unless required by law).'

Roughly a quarter of the page on 'Cookies, Pixels & Similar Technologies' is about Facebook's security interests, a quarter is about the security interests and the convenience of Facebook's users, and the rest is about Facebook's business and other interests. Facebook's 'Community Standards' is a kind of private ordering, imposing Facebook's rules onto its users, generally independent of any existing regulatory environment. Under the heading 'Keeping your account and personal information secure' Facebook states to 'protect your personal information' – a security-only promise –, while demanding from their users to 'not publish the personal information of others without their consent' – a much more privacy-related issue.

4.3 Amazon

Amazon calls its central terms of service 'Conditions of Use', which may become superseded by additional terms for specific Amazon services. Like Google and Facebook's ToS, it explicitly refers to the 'Amazon.com Privacy Notice' for review 'to understand our practices' of information collection, processing and use. Contrary to Google and Facebook's ToS, Amazon's 'Conditions of Use' contain only a few rules about information practices in itself.

The two most important information-related rules refer to the users' sole responsibility 'for maintaining the confidentiality' of his or her account and password and to the prohibition of posting content on Amazon.com that is 'invasive of privacy'.

The first aspect covered by the 'Amazon.com Privacy Notice' is on 'personal information about customers' gathered by Amazon. The company claims personalisation and continual improvement of 'your Amazon experience' to be the purpose of its information collection, processing, and use. Amazon states to collect all information produced by customers using its services or receiving ads by or on behalf of the company, either user input or user interactions, as well as by the users' computers when accessing Amazon.com or

one of its third-party sellers, like connection information, clickstream data and location data. Additionally, Amazon states to receive information ‘about you from other sources’ to be used for social sorting purposes ‘to offer certain credit or financial services to some customers’. Other possible uses mentioned in the ‘Privacy Notice’ are customisation, personalised advertising, and fraud detection.

Amazon does not clarify why it treats cookies in a special section (‘What About Cookies?’). However, Amazon describes how the user may disable cookies in her browser.

Like Facebook, Amazon calls all dissemination of personal information ‘sharing’. Using a ‘privacy=confidentiality’ assertion, Amazon assures its customers that information about them ‘is an important part of our business’, and that the company will not sell it to others. Alongside subsidiaries falling under the same Privacy Notice or one ‘at least as protective’, Amazon shares information about customers with affiliated businesses like those operating stores at Amazon.com, third-party service providers like delivering services, and law enforcement agencies. Amazon states that affiliated businesses receive only ‘information related to those transactions with that third party’, while third-party service providers receive only ‘information needed to perform their functions’, and at least the latter are also purpose-bound.

With respect to the question ‘How Secure Is Information About Me?’, Amazon refers to transmission security measures on the way between Amazon and its customers and requirements on its customers only, but does not mention any security measures either at Amazon itself, affiliated businesses or third-party service providers, or related to transmissions between these players.

For information on the topic of third-party advertisers, Amazon just refers to its ‘Interest-Based Ads’ policy. There, the company simply states that it will use all information available about its customers for personalised advertisements, but will not disclose personal information to advertisers or third-party sites that display these interest-based ads. At the same time, Amazon admits openly and explicitly that these players may infer from users clicking on an interest-based ad that they are ‘part of the group that the ad or content is directed towards’ – an information not widely known nor understood by end-users.

The shortest section in the Privacy Notice refers to the users’ ability to access information about them that is stored by Amazon ‘for the limited purpose of viewing and, in certain cases, updating that information’, but Amazon will ‘usually keep a copy of the prior version for our records.’ So Amazon does not see deletion or use limitations as a viable option for their customers – a practice often criticised by data protection authorities and privacy advocates (Schulzki-Haddouti, 2015).

Scattered remarks in Amazon’s ‘Privacy Notice’ refer to options for ‘opting-out’ Amazon’s widespread surveillance measures, e. g. by turning off cookies in the user’s browser or location services. While Amazon explicitly explains that users ‘can always choose not to provide information’ on Amazon’s website, the company provides no choice to limit its collection of personal information. Instead, the user may only opt for particular – and very limited – use limitations, e. g. not receiving emails from Amazon or not ‘to use personal information that we gather to allow third parties to personalize advertisements we display to you.’

4.4 Apple

Apple has three central terms of services document: one each for its website, iCloud, and all Apple media

services. All three ToS explicitly refer to Apple's privacy policy document. However, all three policy documents also contain rules about Apple's information collection, processing and use. Additionally, Apple has published a letter from its CEO, Tim Cook, to its users and customers on 'Apple's commitment to your privacy' on the company's privacy landing page. Cook states that Apple protects its users' privacy 'with strong encryption, plus strict policies that govern how all data is handled.' In the letter, Cook also refers explicitly to Apple's business model of selling 'great products' as a reason why users should trust the company. He also states that Apple would not sell behavioural profiles to advertisers. On the other hand, there are two loopholes: iAd as a service for advertisers is mentioned explicitly, while Cook keeps quiet about using profiles for Apple's own purposes. And finally, the letter contains two extremely specific statements concerning Apple's cooperation with government agencies: Apple has never worked with any government agency from any country 'to create a backdoor', and that the company has never allowed 'access to its servers' and never will.

Like Amazon, Apple clarifies on its 'Website Terms of Use' (ToU) that users are 'entirely responsible for maintaining the confidentiality' of the information they hold for their account, including their password. This clause is also included in all other Apple policies. The user has to acknowledge and agree that Apple may store any information transmitted while using the website for an unspecified amount of time. The ToU also contains a broad exception clause for disclosing this information to any third parties including government agencies at Apple's sole discretion. While both terms seem to relate to the 'Violation of These Terms of Use' due to their placement, their wording is far too broad to be restricted to cases of ToU violations.

Apple's 'iCloud Terms and Conditions' (TaC) cover a wide range of internet services, 'including storing your personal content (such as contacts, calendars, photos, notes, reminders, documents, app data, and iCloud email) and making it accessible on your compatible devices and computers, and certain location based services'. Since Apple's September 2015 TaC revision, iCloud and all but two of its sub-services like Find My Phone or Backup are turned on by default when setting up a new device running iOS 8 or later, but users may disable particular sub-services or iCloud as a whole. For its services and 'to the greatest extent permissible by applicable law', Apple does not guarantee data integrity nor availability, not even for Backup. Instead, the users are made responsible for their own backup when using Backup. According to the TaC, Apple can 'access, use, preserve and/or disclose your Account information and Content to law enforcement authorities' whenever required or permitted by law, which means that even if the data is kept encrypted on its servers, Apple certainly keeps a master key – a practice that violates every basic security rule.

All Apple's media services – iTunes, App and Book Stores, Apple Music, and Apple News – 'Terms and Conditions' (TaC) are combined in one document, although there is much differentiation within the document concerning the rule governing one, multiple or all services. Until its September 2016 revision, the TaC was primarily, yet exhaustively covering the many different functions and purposes of Apple's recommender system called Genius – an in-house advertising system in all but name. In its current version, the TaC is much less vocal about information practice issues either by Apple itself or by its users, they are often simply presented in passing. Firstly, Apple states that the user is solely responsible for maintaining the confidentiality and security of her Apple ID, and that Apple 'is not responsible for any losses arising from the unauthorised use of your Apple ID.' Secondly, Apple grants itself the right to 'monitor your use of the

Service and Content’ for checking compliance with the usage rules. Thirdly, the recommender system is still used widely by Apple ‘based on your downloads, purchases and other activities’, but not mentioned by name, and still without a possibility for the user to prevent Apple from collecting and storing this information in the first place – users ‘may [only] opt out from receiving such recommendations.’ And last but not least, Apple forbids the use of its services to ‘post personal, private or confidential information belonging to others.’

Apple’s ‘Privacy Policy’ (PP) is subdivided into thirteen sections without any consistency. There are sections following the distinguishable steps of modern information processing such as collection and use, disclosure, or deletion. But the policy also contains sections referring to particular groups of users (children, international users), specific security measures by Apple, or even particular technologies like location-based services or cookies and other tracking technologies. This structure apparently is designed to mislead the reader: after the first section ‘Collection and Use of Personal Information’, the reader learns that more information about the collection and use of personal information is scattered all over the policy, most concentrated in the ‘Cookies and Other Technologies’ section. Furthermore, the company provides only some examples in the ‘Collection and Use’ section. The examples are arranged in two groups illustrating which information Apple collects and how it uses the data. Both refer to information that is explicitly shared by users with the company, but the former remains silent about information collected in any other way. The latter includes two overly broad uses: first, to ‘create, develop, operate, deliver, and improve our products, services, content and advertising, and for loss prevention and anti-fraud purposes’, and second, partially reiterating the first one, ‘for internal purposes such as auditing, data analysis, and research to improve Apple’s products, services, and customer communications’. It’s hard to tell if there could be any business model or use case at all not covered by these two clauses. While the first section of the policy covers the collection and use of personal information, the second section covers non-personal information which Apple considers to be collectable, usable, transferable, and disclosable for any purpose. Surprisingly, Apple treats unique device identifiers and IP addresses as non-personal information, even though the device identifiers of most Apple devices are certainly associated with accounts which are themselves associated with Apple IDs, and therefore well-known to Apple. The company only treats the aforementioned information as personal information if it does combine them with other personal information, or – as stated in the ‘Cookies and Other Technologies’ section – if the information is considered personal information by local law. But this distinction has no consequences at all: as users have to consent to Apple’s privacy policy anyway, Apple may lawfully collect as much information about user behavior as it wants; users may opt-out from receiving targeted ads based on information collected by ‘cookies and other technologies’, but this applies anyway, whether this information is deemed to be personal or not.

Apple also grants itself the right to share ‘certain personal information’ with third parties for them ‘to provide or improve our products, services and advertising’. These third parties are not allowed to use this information ‘for their marketing purposes’. Additionally, Apple may share personal information in response to ‘public and governmental authorities within or outside your country of residence’ or if the company determines ‘that for purposes of national security, law enforcement, or other issues of public importance, disclosure is necessary or appropriate’. Apple does not differentiate between warrant-based and warrantless searches, nor provides criteria for its decision-making, nor states what procedural requirements have to be met.

The policy states that Apple will retain personal information as long as permitted by law, at least if not requested by users to delete the information.

Such narrow understanding is also guiding Apple in providing users with access to their personal information, which may be declined if Apple deems the user's request 'extremely impractical' or 'frivolous'. At least, Apple also states to be very helpful to people who want to complain about the company's understanding of personal information or its information practices: 'If you ask us, we will endeavor to provide you with information about relevant complaint avenues which may be applicable to your circumstances.'

Apple's 'Our Approach to Privacy' page attempts to describe 'powerful safeguards [built] into our operating systems, our apps, and the devices themselves'. Unfortunately, most of them are security – to 'keep your personal information safe' –, not privacy mechanisms. For example, iMessages are protected by end-to-end encryption, which neither third parties nor Apple can decrypt 'when it's in transit between devices', but they are backed up in iCloud by default when not in transit anymore – for which Apple retains the keys. Therefore, iMessages are not protected against Apple's information interests – or third-party interests which Apple satisfies – if not both communication partners turned off iCloud Backup. On the other hand, Apple's description of Maps is reasonably convincing that its usage of random anonymised rotating identifiers protects users from Apple. In most cases, however, for example in News, Apple just uses service-specific profiling, promising its users not to link those different profiles together. Throughout the text, Apple uses the concepts of safety, security and privacy rather interchangeably. The same holds true for Apple's 'Manage Your Privacy' page with 'information about powerful features that help you make your devices and data secure, along with tips for avoiding phishing scams and keeping your account safe'. It's mostly about security, and even the privacy management mechanisms address primarily privacy interests against third parties.

5 PRIVACY FRAMING AND BUSINESS MODELS

The following section will present an analysis of the relationship between the companies' privacy framings and their business models. The analysis is not exhaustive as it does not cover all of the four companies' business fields, e. g. Google Fiber or Amazon Web Services.

An overwhelming part of Google's revenue comes from its advertising programs, AdWords, AdSense and DoubleClick. From a business model point of view, the purpose of Google's other services, including Search, Google+ or YouTube, is to attract users to its websites to stay there as long as possible, and make them see and click as many ads as possible. Most of Facebook's revenue derives from advertising, as well. The social networking site which Facebook operates, plays pretty much the same role for the company's revenue as in Google's case. Within the scope of this study, Amazon is an internet-based retailer, selling almost everything – books, electronic media, but also furniture, toys and even food. Additionally, the company runs the platform Marketplace, enabling third-party sellers to offer new and used items on Amazon's platform. Amazon's revenue in these business fields comes from the company's own sales, and sales and subscription fees for third-party sellers. Apple is a technology company, designing, developing, and selling consumer electronics, software, and online services like the iTunes Store, the App Store, and iCloud. Apple is the world's second-largest information technology company by revenue, its iTunes Store

is the world's largest music retailer. About 60% of its revenue comes from the sale of iPhones, approximately 6% from iTunes Store, App Store, and iBooks Store.

Many different stakeholders are mentioned in the privacy policies – companies either using ‘we’ or their names, and their users and/or customers. All privacy policies include references to subsidiaries and third-party companies working on behalf of the company. Some policies refer specifically to family members, i. e., for example Apple's privacy policy. Social network operators also refer to third parties using their platforms, oftentimes blurring the lines between individuals and organisations in this regard. The same holds true for most other mentions of third parties (often simply denominated ‘others’), advertising companies being the rare exception of this blurring. Dedicated attackers are seldom mentioned, and then mostly by referring to particular actions attributed to them like spamming or identity theft. In all privacy policies analysed, special consideration is given to state actors like governments, law enforcement agencies or intelligence services.

Information-related interests and purposes are not clearly attributed to all the players mentioned in the privacy policies, not even to the companies themselves. Most attributions are only examples or too broad to be meaningful. The consequences are substantial: collected information is rarely bound to a specific purpose and used only for this purpose. Most collected information is to be used for all purposes specified anywhere in any privacy policy. With definitions of purposes such as ‘to design new services and products’ or ‘to improve our products, services, content and advertising’, as found in all privacy policies analysed, there can be neither data minimisation, nor time limits for data retention, nor purpose-binding in any meaningful sense. Google, Amazon and Apple also differentiate between advertisements and recommendations in their policies. The former refers to third-party ads only, while ads promoting the companies' own products and services are simply called ‘recommendations’. The same holds true for targeting and personalisation: personalised advertising is called ‘targeted’ or ‘tailored’, while targeted recommendations are framed as ‘personalised’ or ‘customised’. In both cases, companies attempt to frame particular information practices – their own practices – as less threatening or intrusive than others – practices by third parties –, even if they are the same with similar consequences for the privacy of their users. Thus, it's not surprising then that a company like Apple can assure its customers that it would not ‘monetise’ their behavioural profiles – it's simply the result of successfully framing the company's own ads as ‘recommendations’.

Concerning particular practices, all four companies focus predominantly on sharing and disclosure when depicting privacy-sensitive actions. Usually, they thereby refer to actions of users and companies alike vis-à-vis third parties, seldom to users' actions vis-à-vis the companies. This is kind of a deception, depicting these companies more as an extension of their users and customers than as separate entities. Apple does not monetise its users' chats or messages as the company's CEO promised in his letter to Apple's customers, but it certainly does monetise their media uses. None of the companies sells profiles to third parties, but they all do create behavioural profiles for their own purposes. The often repeated statement, e. g. by Amazon, ‘we are not in the business of selling it to others’ is therefore at least misleading.

The definitions of personal information used in the policies seem as narrow as possible to enable individually-targeted advertising or personalised recommendations without using information that would fall under these definitions.

In general, threats to users' and customers' privacy interests are depicted as more severe in all privacy policies if they originate from third parties. Apple, for example, even warns its customers explicitly: 'Please take care when using these features' of sharing information with others. No company would include a warning of this kind against its own information practices and uses. The most extreme case is Facebook: the company describes its own information practices in its 'Data Policy', while the 'Privacy Basics' page only refers to informational relationships between users and third parties, be it other users, companies, or strangers.

6 CONCLUSIONS AND FUTURE WORK

All four companies try to prevent being seen as something other than the guardian of their users' privacy. Their policies do not contain descriptions or explanations which would suggest that the companies are a threat to their users' privacy. Instead, even when and where the companies recognise their involvement in possible privacy infringements, they depict themselves as an extension of the users' actions or as a mediator.

The companies' examples of how they use personal information and for what purposes are at least misleading. First, they are neither sufficient nor adequate to inform users about the companies' information practices. Second, they only cover less intrusive practices and purposes which most people won't find threatening or at least find acceptable, like fraud prevention. And third, they use deceptive language like 'recommendations' instead of 'ads' to describe the companies' practices. None of the framings of the privacy issue in the policies analysed in this study is based on an established privacy, surveillance or data protection theory. The companies' self-commitment to not infringe upon their users' privacy is therefore not verifiable in any meaningful sense, because as they frame 'privacy' in a way that fits best their business interests, their information practices would virtually never represent a violation of this 'privacy'.

Finally, the role of power in the information processing ecosystem is completely absent from all privacy policies analysed. None of the companies reflects upon being the much more powerful part in a very imbalanced power relationship with its customers and users – the companies, not the users, control the means of production of decisions about users. But this comes as no surprise, because power is a concept that does not fit easily into a global privacy debate focusing primarily on the freedom of autonomous and equal individuals to make utility-maximising decisions in informational relationships with other private parties, while power relations are at best discussed if public and governmental authorities are involved. It is therefore not a contradiction that the same companies presenting their users and customers with privacy policies lacking any substantive protection of the users and customers' privacy from the companies' information practices very publicly call for a limitation of the states' power to collect and use personally identifiable information, e.g. by joining pressure groups like the Global Network Initiative.

This study can only be the first step in a much broader analysis of the framing of privacy in terms of service and privacy policies of companies around the globe with respect to their particular business models, but also with respect to existing philosophical, sociological, legal and informational privacy, surveillance and data protection theories. A follow-up study would most probably need to include more companies, either from the same or from completely different fields, either with similar or highly different business models, but of different sizes to clarify whether the many similarities between the policies, which this study uncovered, are but a consequence of all four companies dominating their respective markets. Additionally, all four

companies have a similar cultural background. The question arises whether the framing of privacy is different in companies of similar size and market dominance but with different cultural backgrounds. And third, it remains an open question whether the fact that all privacy policies have been edited by lawyers has levelled out all differences which might have existed before. It might also be possible that in modern information capitalism, all companies are forced to create profiles as exhaustive as possible of their users and customers, to monetise the users' behaviour, to commodify them, while maintaining a certain simulation of privacy protection to satisfy the expectations of members of a bourgeois society. The question of what guides or even determines the framing of privacy in terms of service and other policy documents of private businesses which govern user expectations and business practices alike is still not conclusively answered.

APPENDIX: LIST OF POLICY DOCUMENTS

All documents were last accessed September 30, 2016.

Google

- Terms of Service: <https://www.google.com/intl/en/policies/terms>.
- Privacy Policy: <https://www.google.com/intl/en/policies/privacy/>.
- Key terms: <https://www.google.com/intl/en/policies/privacy/key-terms/>.
- Technologies and Principles: <https://www.google.com/intl/en/policies/technologies/>.
- Self Regulatory Frameworks: <https://www.google.com/intl/en/policies/privacy/frameworks/>.
- Explore easy-to-use safety tools: <https://www.google.com/intl/en/safetycenter/tools/>.
- FAQ: <https://www.google.com/intl/en/policies/faq/>.

Facebook

- Terms of Service: <https://www.facebook.com/legal/terms>.
- Data Policy: https://www.facebook.com/full_data_use_policy.
- Community Standards: <https://www.facebook.com/communitystandards>.
- Facebook Help Center | Cookies, Pixels & Similar Technologies: <https://www.facebook.com/help/cookies>.
- Facebook Privacy Basics: <https://www.facebook.com/about/basics>.

Amazon

- Conditions of Use: https://www.amazon.com/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=508088.
- Privacy Notice: https://www.amazon.com/gp/help/customer/display.html/ref=hp_left_v4_sib?ie=UTF8&nodeId=201909010.
- Interest-Based Ads: <http://www.amazon.com/b/?&node=5160028011>.

Apple

- Apple Website Terms of Use: <http://www.apple.com/legal/internet-services/terms/site.html>.
- iCloud Terms and Conditions: <http://www.apple.com/legal/internet-services/icloud/en/terms.html>.
- Apple Media Services Terms and Conditions: <http://www.apple.com/legal/internet-services/itunes/us/terms.html>.
- Apple Privacy Policy: <http://www.apple.com/privacy/privacy-policy/>.
- Privacy: <http://www.apple.com/privacy/>.
- Our Approach to Privacy: <http://www.apple.com/privacy/approach-to-privacy/>.
- Manage Your Privacy: <http://www.apple.com/privacy/manage-your-privacy/>.
- Government Information Requests: <http://www.apple.com/privacy/government-information-requests/>.

REFERENCES

- Anderson, Ross (2008) *Security Engineering: A Guide to Building Dependable Distributed Systems*. Vol. 2. New York: John Wiley & Sons.
- Borghi, Maurizio, Federico Ferretti and Stavroula Karapapa (2013) 'Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK', *International Journal of Law and Information Technology* 21(2): 109–153.
- Cohen, Julie E. (2019) *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford: Oxford University Press.
- Earp, Julia B., Annie I. Antón and Olli Jarvinen (2002) 'A Social, Technical and Legal Framework for Privacy Management and Policies', *Americas Conference on Information Systems (AMCIS)*: 605–612.
- Earp, Julia B. et al. (2005) 'Examining Internet privacy policies within the context of user privacy values', *IEEE Transactions on Engineering Management* 52(2): 227–237.
- Friedewald, Michael., Ina Schiering, Nicholas Martin and Dara Hallinan (2022) 'Data Protection Impact Assessments in Practice', in S. Katsikas et al. (eds.) *Computer Security. ESORICS 2021 International Workshops. CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, Germany, October 4–8, 2021, Revised Selected Papers*. Springer, Cham: 424–443.
- Gallie, Walter Bryce (1956) 'Essentially Contested Concepts', *Proceedings of the Aristotelian Society. New Series* 56: 167–198.
- Gandy, Jr., Oscar H. (1993) *The Panoptic Sort*. Boulder: Westview Press.
- Gavison, Ruth (1980) 'Privacy and the Limits of Law', *The Yale Law Journal* 89(3): 421–471.
- Guyonn, Jessica (2014) 'Privacy watchdog files complaint over Facebook study', *USA Today*, 3 July. URL: <http://www.usatoday.com/story/tech/2014/07/03/facebook-emotion-study-complaint-epic/12157471/>.
- Hansen, Marit (2008) 'Linkage Control – Integrating the Essence of Privacy Protection into Identity Management Systems', in P. Cunningham and M. Cunningham (eds) *Collaboration and the Knowledge Economy: Issues, Applications, Case Studies*. Amsterdam: IOS Press: 1585–1592.
- (2009) 'Putting Privacy Pictograms into Practice – a European Perspective', in Stefan Fischer, Erik Maehle and Rüdiger Reischuk (eds.) *INFORMATIK 2009: Im Focus das Leben*. Bonn: Gesellschaft für Informatik: 1703–1716.
- Hansen, Marit, Meiko Jensen and Martin Rost (2015) 'Protection Goals for Privacy Engineering', *Proceedings of the International Workshop on Privacy Engineering (IWPE)*, IEEE eXplore. URL: <https://iee-security.org/TC/SPW2015/IWPE/2.pdf>.
- Haynes, Allyson W. (2007) 'Online Privacy Policies: Contracting Away Control Over Personal Information', *Penn State Law Review* 111: 587–624.
- Hoffman, Lance J. and William F. Miller (1973) 'Getting a Personal Dossier from a Statistical Data Bank', in Lance J. Hoffman (ed.) *Security and Privacy in Computer Systems*. Reprint from: Datamation, 1970. Los Angeles: Melville Publishing Company: 289–293.
- Hoffmann, Bernhard (1991) *Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes*. Baden-Baden: Nomos Verlagsgesellschaft.
- Hung, Patrick C. K. (2005) 'Towards a Privacy Access Control Model for e-Healthcare Services', in *Third Annual Conference on Privacy, Security and Trust*, October 12–14, 2005 Proceedings.
- Jørgensen, Rikke Frank (2018) 'Framing human rights: exploring storytelling within internet companies', *Information, Communication & Society* 21(3): 340–355.
- Kamarinou, Dimitra, Christopher Millard and W Kuan Hon (2015) *Privacy in the Clouds: An Empirical Study of the Terms of Service and Privacy Policies of 20 Cloud Service Providers*. Queen Mary School of Law Legal Studies Research Paper No. 209/2015.

- Kang, Jerry (1998) 'Information Privacy in Cyberspace Transactions', *Stanford Law Review* 50(4): 1193–1294.
- Kelley, Patrick Gage et al. (2009) 'A "Nutrition Label" for Privacy', *Proceedings of the 5th Symposium on Usable Privacy and Security*. ACM, Article 4.
- Kuczerawy, Aleksandra and Fanny Coudert (2011) 'Privacy Settings in Social Networking Sites: Is It Fair?', in Simone Fischer-Hübner et al. (eds.) *Privacy and Identity Management for Life*. Berlin: Springer: 231–243.
- Livingston, Jared S. (2011) 'Invasion contracts: The privacy implications of terms of use agreements in the online social media setting', *Albany Law Journal of Science and Technology* 21: 591–636.
- Lyon, David (ed.) (2003) *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*. London: Routledge.
- Marx, Gary T. (2015) 'Surveillance Studies', in James D. Wright (ed.) *International Encyclopedia of the Social & Behavioral Sciences*. 2nd ed. Amsterdam: Elsevier: 733–741.
- Medzini, Rotem (2016) 'Prometheus Bound: An Historical Content Analysis of Information Regulation in Facebook', *Suffolk University Journal of High Technology Law* 16: 195–293.
- Müller, Paul J. (1975) 'Funktionen des Datenschutzes aus soziologischer Sicht', *Datenverarbeitung im Recht* 4: 107–118.
- Nissenbaum, Helen (2004) 'Privacy as contextual integrity', *Washington Law Review* 79: 101–139.
- Ohm, Paul (2010) 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization', *UCLA Law Review* 57: 1701–1777.
- Ortmann, Steffen, Peter Langendörfer and Michael Maaser (2007) 'Enhancing Privacy by Applying Information Flow Modelling in Pervasive Systems', in Robert Meersman, Zahir Tari, and Pilar Herrero (eds.) *On the Move to Meaningful Internet Systems 2007: OTM 2007 Workshops*. Berlin: Springer: 794–803.
- Podlech, Adalbert (1976) 'Gesellschaftstheoretische Grundlage des Datenschutzes', in Rüdiger Dierstein, Herbert Fiedler, and Arno Schulz (eds.) *Datenschutz und Datensicherung*. Köln: J. P. Bachem Verlag: 311–326.
- Pohle, Jörg (2015). 'Transparenz und Berechenbarkeit vs. Autonomie- und Kontrollverlust: Die Industrialisierung der gesellschaftlichen Informationsverarbeitung und ihre Folgen', *Mediale Kontrolle unter Beobachtung* 4(1). URL: <https://www.medialekontrolle.de/wp-content/uploads/2016/03/Pohle-Joerg-2016-05-01.pdf>.
- (2016). 'Die kategoriale Trennung zwischen "öffentlich" und "privat" ist durch die Digitalisierung aller Lebensbereiche überholt – Über einen bislang ignorierten Paradigmenwechsel in der Datenschutzdebatte', in Michael Plöse et al. (eds.) *Worüber reden wir eigentlich? Festgabe für Rosemarie Will*. Berlin: Humanistische Union.
- Reay, Ian, Scott Dick and James Miller (2009) 'A large-scale empirical study of P3P privacy policies: Stated actions vs. legal obligations', *ACM Transactions on the Web (TWEB)* 3(2), Article 6.
- Reidenberg, Joel R. et al. (2015) *Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding*. Fordham Law Legal Studies Research Paper No. 2418297; 2014 TPRC Conference Paper; Berkeley Technology Law Journal, Vol. 30, 2015; Fordham Law Legal Studies Research Paper No. 2418297. URL: <http://ssrn.com/abstract=2418297>.
- Rizk, Ramzi, Seda F Gürses, and Oliver Günther (2010) 'SNS and 3rd Party Applications Privacy Policies and their Construction of Privacy Concerns', *ECIS 2010 Proceedings*, Paper 143. URL: <http://aisel.aisnet.org/ecis2010/143>.
- Rossum, Henk van et al. (1995) *Privacy-Enhancing Technologies: The Path to Anonymity*. Den Haag: Information and Privacy Commissioner / Ontario, Canada & Registratiekamer, The Netherlands.
- Rotenberg, Marc (2001) 'Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)', *Stanford Technology Law Review* 1. URL: <http://stlr.stanford.edu/pdf/rotenberg-fair-info-practices.pdf>.
- Rubinstein, Ira and Nathan Good (2012) *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*. NYU School of Law, Public Law Research Paper 12-43.
- Schneier, Bruce (2004) *Secrets and lies: digital security in a networked world*. Paperback Edition. Indianapolis: Wiley Publishing.
- Schulzki-Haddouti, Christiane (2015). 'Unbefristete Amazon-Speicherpraxis: Kritik an Luxemburger Datenschutz-

- Behörde', *heise online*, 31 July. URL: <https://heise.de/-2765721>.
- Shmatikov, Vitaly (2011) 'Anonymity Is Not Privacy', *Communications of the ACM* 54(12): 132.
- Simitis, Spiros (1987) 'Reviewing Privacy in an Information Society', *University of Pennsylvania Law Review* 135: 707–746.
- Solove, Daniel J. (2006) 'A Taxonomy of Privacy', *University of Pennsylvania Law Review* 154(3): 477–560.
- Steinmüller, Wilhelm et al. (1971) *Grundfragen des Datenschutzes*. Expertise on behalf of the German Ministry of the Interior, BT-Drs. VI/3826, Appendix 1.
- Sweeney, Latanya (2002) 'Achieving k-Anonymity Privacy Protection Using Generalization and Suppression', *International Journal of Uncertainty Fuzziness and Knowledge-Based Systems* 10(5): 571–588.
- U.S. Department of Health, Education, and Welfare (1973) *Records, Computers, and the Rights of Citizens*. Cambridge, MA: The Massachusetts Institute of Technology.
- Van Loo, Rory (2022) 'Privacy Pretexts', Preprint available at: <https://ssrn.com/abstract=4048919>.
- Vries, Katja de (2013) 'Privacy, due process and the computational turn: A parable and a first analysis', in Mireille Hildebrandt and Katja de Vries (eds.) *Privacy, Due Process and the Computational Turn*. Abingdon: Routledge: 9–38.
- Wagner, Isabel (2022) 'Privacy Policies Across the Ages: Content and Readability of Privacy Policies 1996–2021', *arXiv preprint arXiv:2201.08739*.
- Waldman, Ari Ezra (2020) 'Privacy Law's False Promise', *Washington University Law Review* 97: 773–834.
- Ware, Willis H. (1967) 'Security and privacy: similarities and differences', *Proceedings of the April 18-20, 1967, spring joint computer conference. AFIPS '67 (Spring)*. Atlantic City, NJ: ACM: 287–290.
- Westin, Alan F. (1967) *Privacy and Freedom*. New York: Atheneum.