Information Systems Frontiers
https://doi.org/10.1007/s10796-019-09974-2

How Data Protection Regulation Affects Startup Innovation

Nicholas Martin [1] · Christian Matt [2] · Crispin Niebel [3] · Knut Blind [1,3]

Abstract
While many data-driven businesses have seen rapid growth in recent years, their business development might be highly contingent upon data protection regulation. While it is often claimed that stricter regulation penalizes firms, there is only scarce empirical evidence for this. We therefore study how data protection regulation affects startup innovation, exploring this question during the ongoing introduction of the EU General Data Protection Regulation (GDPR). Our results show that the effects of data protection regulation on startup innovation are complex: it simultaneously stimulates and constrains innovation. We identify six distinct firm responses to the effects of the GDPR; three that stimulate innovation, and three that constrain it. We furthermore identify two key stipulations in the GDPR that account for the most important innovation constraints. Implications and potential policy responses are discussed.

Keywords Data protection regulation · Privacy regulation · GDPR · Innovation · Startups · Compliance innovation · Regulation-exploiting innovation

1 Introduction

Firms increasingly exploit data to optimize products and processes, and innovate new business models (Baesens et al. 2016; Hartmann et al. 2016). Yet use of personal data can conflict with consumers' and employees' privacy expectations (Carpenter et al. 2018), creating complex challenges for individuals, groups and societies (Kim et al. forthcoming). Data protection law[1] tries to resolve these conflicts by defining rules for what firms may legally do with data.

Both individuals' privacy perceptions and the substantive content of data protection law (privacy law) vary substantially across countries (Cho et al. 2009; Dinev et al. 2006). For instance, Europe has stricter and more systematic data protection legislation regulation than the U.S. (Clemons & Banattar 2018). This for instance

[1] In the USA and other Anglo-Saxon countries the term "privacy" is commonly used, while in Europe the term "data protection" predominates. There are subtle philosophical and jurisprudential differences between the two concepts, but for most practical purposes the two are largely identical (for discussion see De Hert and Gutwith 2006). For linguistic variation we use the two terms interchangeably.

✉ Christian Matt
christian.matt@iwi.unibe.ch

Nicholas Martin
nicholas.martin@isi.fraunhofer.de

Crispin Niebel
c.niebel@tu-berlin.de

Knut Blind
knut.blind@tu-berlin.de

[1] Fraunhofer ISI, 76139 Karlsruhe, Germany

[2] University of Bern, Institute of Information Systems, 3012 Bern, Switzerland

[3] Technische Universität Berlin, Chair of Innovation Economics, 10587 Berlin, Germany

Published online: 18 November 2019

relates to the conditions under which data can be processed[2] by firms, what counts as personal data, or who needs to be notified in case of data breaches (PWC 2016). The differences between European data protection law and the laws of other countries became even more pronounced after the EU General Data Protection Regulation (GDPR) came into force in May 2018, replacing the 1995 EU Data Protection Directive (DPD). In particular, the GDPR imposed dramatically higher fines for non-compliance, expanded the definition of personal data, and tightened the criteria for what counts as user consent.[3]

Companies often claim that stricter data protection regulation puts them at a disadvantage in relation to firms in countries with laxer regulation (Wallace & Castro 2018), pointing to possible trade-offs between privacy protection and the promotion of competitiveness. However, others argue that stricter regulation may be needed to restore trust in the digital economy (Economist 2018). Beyond the firm level, this question is important for societies and policy makers, given the possible effects on domestic firms' global competitiveness. Better understanding of how privacy regulation impacts firms is therefore important for policy makers seeking to protect both individuals' privacy and firms' competitiveness.

While the appropriate stringency level for data protection regulation remains contested, the question of how and to what extent such regulation affects firm performance has received only limited scholarly attention (Morlok et al. 2018). Previous research that has studied country or industry-wide effects of data protection regulation on firm performance has often taken data protection regulation effects as a monolithic black box, providing high-level insights but without identifying concrete impacts and responses at the firm level, or identifying concrete causes of these effects. Yet it is unlikely that the effects of data protection regulation are uniform, since the types of data firms employ, the ways they use it and their relations to end users vary substantially. Given the central role of personal data in many business models today, scholars, regulators and entrepreneurs require a better understanding of the issue, in particular since the GDPR has recently come into effect and might have led to substantial changes in this domain. To provide insightful answers, we focus our analysis on a particular company type and a particular corporate function: We analyze how data protection regulation affects corporate innovation, focusing on product and service innovation with data-based startups in Germany. We ask the following research questions:

- *How does data protection regulation affect innovation among startups? Does it primarily constrain or stimulate the development of new products and services and thus increase or decrease overall innovation?*
- *What are the concrete responses that firms choose in order to deal with any constraints or opportunities that data protection regulation creates for them?*

We seek to answer these questions with a two-stage approach consisting of semi-structured interviews: First we interviewed lawyers and other intermediaries of the startup ecosystem to obtain insights into the regulatory framework conditions (enforcement levels, compliance strategies, etc.) as well as a broad overview of data protection regulation's apparent effects on innovation. Second, we interviewed startups directly to obtain more fine-grained information on individual company perceptions and their responses.

Our study extends the literatures on the economics of privacy and of regulation. We exploit a unique moment in time: by conducting the intermediary interviews just before and just after the GDPR came into force, we still captured the effects on innovation of the previous data-protection regime, since respondents' impressions at that point were mostly formed by the old Directive. By conducting the startup interviews eight months after the GDPR came into force, we obtain first insights into the GDPR's effects and can compare these to the old Directive.

The paper is structured as follows: The next section discusses the literature on regulation's effects on firm innovation. Building on this, Section 3 develops a basic conceptual framework to explain how firms may respond to data protection regulation and how this would impact innovation. We use this to guide our research and will extend and refine it in light of research results. Section 4 describes our research methodology and data. Section 5 presents the results. Section 6 discusses implications for further research and for policy. Section 7 concludes.

2 Effects of Regulation on Firm Innovation

Regulation refers to any general form of "coercive rule setting" by governments to influence market activity and economic actors' behavior (Blind et al. 2017). Scholars and practitioners distinguish three types of regulation; viz. economic regulation such as anti-trust; social regulation (e.g. consumer and environmental protection); and institutional regulation (rules on liability, bankruptcy, etc.) (OECD 1997). We consider data protection

[2] "Processing" is a generic term to describe all handling of data, from collection through to erasure.

[3] We use the terms data protection/privacy "regulation" and (for linguistic variation) "law" to refer to data protection legislation in general. When discussing specific pieces of legislation like the GDPR, the Directive, or the German Federal Data Protection Law we refer to them by their full names or abbreviations.

regulation to be a type of social regulation, similar to consumer protection.[4] European data protection laws, such as the GDPR, the Directive and the national laws[5] outline rules for the conditions under which people's data can be legitimately processed. It aims to protect people from two threats. Firstly, from irregular attacks on people's data by criminal outsiders ("hackers") and rogue insiders acting in contravention of their organization's rules. Secondly, from people's data being processed illegally by organizations acting in accordance with their internal (but illegal) rules and objectives. Data protection law seeks to achieve the first end mainly through IT security. The second end is achieved by mandating extensive process controls. These include controls on the conditions under which data can be processed legally (e.g. by stipulating that processing needs a legal basis, like consent) and under which it may be transferred abroad. Further controls include providing people with rights vis-a-vis data controllers, and by stipulating certain organizational and processing measures (e.g. data protection officers, breach notifications). Almost no processing is illegal per se; rather, legality depends on following the relevant stipulated processes.

Empirical research on the impact of social regulation on innovation and economic performance has focused primarily on the effects of environmental regulation, but has been unable to derive definitive predictions (Ambec et al. 2013; Kozluk and Zipperer 2014). On the one hand, regulation imposes compliance costs on firms, sapping resources otherwise available for productive activities, such as innovation, or raising entry barriers, thus reducing competition and incentives for innovation (e.g. as argued by Blind 2012). If regulation prohibits or obstructs the deployment of certain technologies, promising developmental trajectories may be foreclosed. However, regulation can also provide additional incentives for innovation, leading to the creation of new technologies, products and markets, and the discovery of overlooked efficiencies (the so-called Porter Hypothesis, Porter and van der Linde 1995). If other countries copy a regulation, early adopters may enjoy first-mover advantages in export markets. Regulation can foster consumer trust, thereby increasing demand for new technologies.

[4] The GDPR includes elements of more conventional economic regulation, in particular the "right to data portability", which was added to the GDPR to address anti-trust concerns. This is a novelty for data protection law. While the "right to data portability" can be derived from the basic principles and jurisprudence of European data protection law, this right was not previously codified in extant data protection laws. See Hallinan 2018, in particular Chapters 12-14.

[5] The relationship between EU legislation (GDPR, Directive) and national legislation is complex. Basically, EU legislation relies on national laws for implementation. Thus Germany's Federal Data Protection Law translates the GDPR into national law. EU law mostly takes precedence over national law; i.e., if a court finds that the national law does not fully implement the GDPR (e.g. by changing a given stipulation), the GDPR takes precedence.

Corresponding to this theoretical indeterminacy, empirical findings have been mixed. According to several literature reviews in the environmental and energy field, regulation has had largely though not unanimously positive effects on innovation (Ambec et al. 2013; Blind, 2016; Kozluk and Zipperer 2014). Blind (2012) finds that stricter product and environmental regulation has a significant positive effect on patenting intensity, confirming earlier findings by Rennings and Rammer (2011), who also reveal that regulation-driven innovations are as successful in the market as other innovations. Using data from the 2005 UK Innovation survey, D'Este et al. (2012) find that of four possible barriers to innovation analyzed, regulation was the least problematic. Case studies find that by establishing Germany as a lead market for environmental and new energy technologies, regulation conferred first-mover advantages on local companies, thereby developing new export industries (Blind et al. 2004; Walz et al. 2008). However, scholars have also identified cases where regulation impacted innovation negatively. Blind et al. (2004) find that the EU's strict regulation of genetically modified organisms amounted to a virtual "moratorium on the[ir] commercialization", prompting a substantial reduction in innovation activity. While more stringent regulation of pesticides prompted firms to develop less toxic pesticides, rising compliance costs reduced overall resources available for innovation, leading to a reduction in the number of developed pesticides (Ollinger & Fernandez-Cornejo 1998).

In general, the effects on innovation are highly sensitive to the characteristics of specific regulations and industries (Blind 2016). The time frame may also be important: Negative effects may predominate in the short-term as new regulation disrupts existing structures of production and ways of doing things, while positive, innovation-stimulating effects might only show up in the medium term, since the time to market of innovations starting from research and development take time and depend heavily on the characteristics of the technology (Ambec et al. 2013, Bourke & Roper 2017).

Unfortunately, there has been little research on data protection regulation's effects on innovation. Some work assesses the EU Data Protection and ePrivacy Directives and Regulations (Christensen et al. 2013; Deloitte 2013; London Economics 2017; Ramboll Management 2005; Hildebrandt & Arnold 2017). These studies were mostly commissioned by stakeholders, such as the EU Commission or industry associations. They are mostly prospective, trying to predict future macro-economic effects, but they come to very divergent conclusions, ranging from multi-billion Euro gains to multi-billion Euro losses – innovation, however, is only addressed in passing. Also academic research on the topic is still rare. Goldfarb and Tucker (2011) study the impact of the 2002 EU ePrivacy Directive on advertising effectiveness. They find that advertising effectiveness declined by 65%, and attribute this to barriers that the Directive supposedly created to demographic

targeting. This contrasts rather sharply with the perceptions of some European regulators, who believe that the Directive was never effectively enforced.[6] Campbell et al. (2015) have shown theoretically that stringent privacy regulation may disproportionately damage small companies, leading to more oligopolistic market structures. There is related literature on how large Internet firms bypass privacy regulation or abuse monopoly power, but this mostly focuses on market dominance and competitiveness, rather than regulatory impacts on innovation (Clemons & Madhani 2010). Khansa and Liginlal (2007) find that US information security regulation stimulated demand for IT-security products, and identify a correlation between this demand and R&D expenditure at leading IT-security equipment suppliers, suggesting increased innovation. However, they do not control for alternative causes of growing R&D budgets or examine how regulation affected innovation at the observed companies. Implementing privacy measures may increase consumers' usage of digital products and services (Albashrawi & Motiwalla, forthcoming), thus potentially giving firms that implement privacy measures a competitive advantage (Enzmann & Schneider 2005). However, many studies in this field usually take on an individual user perspective – focusing mostly on user perceptions or knowledge about privacy (e.g. Matt & Peckelsen 2016; Youn 2009) – or they assume a more technological system development perspective (Sun & Upadhyaya 2015). These studies often also miss a firm level perspective when assessing the effects of privacy regulation on innovation, or they do not link the effects of data protection regulation to firm performance. In short, there is still little empirical evidence on privacy regulation's effects on innovation.

3 Developing a Conceptual Framework for Firm Responses to Privacy Regulation

/To understand how data protection regulation may affect innovation, we develop a basic conceptual framework of regulation's effects on companies' innovation choices. Drawing on Blind et al.'s (2017) definition of regulation as "coercive rule[s]" set by government to shape market activity, we theorize that companies whose activities fall within the regulation's scope should ordinarily experience it as a *constraint* on their choices, since it limits what they can legally do, e.g. what they can legally innovate. Thus executives with ideas for new or improved products may discover that privacy regulation limits what they can legally develop or implement, but how will companies faced with regulatory constraint respond? Drawing on Stewart (2010) we argue that they have three basic choices:

- *Product Abandonment:* They can abandon the problematic product or idea to focus on others, that face fewer regulatory restrictions.
- *Compliance Innovation:* They can innovate changes, to make the idea/product compliant, while preserving its basic architecture and value-proposition, e.g. by making default settings more privacy-friendly, or using anonymized data instead of personally-identifiable information. While we conceptualize compliance innovation as primarily about product design (i.e., own engineering work), it can also involve working with new suppliers to ensure that the final product is only built from regulation-compliant components and service.[7]
- *Strategic Non-compliance*: They can deliberately contravene the regulation, at the risk of running afoul of the authorities and facing punitive consequences (fines, closure, etc.)

Which of these three responses firms choose is likely to depend on a mix of internal and external factors, including their technological and financial capabilities, the relative technological and financial easiness of the innovation needed to achieve compliance, the expected level of market demand for regulation-compliant products (which may be low if achieving compliance impairs functionality or raises prices), and the expected level of regulatory enforcement. The regulation's detailed stipulations may impact firm choice and outcomes, too: If regulation is very onerous, it may foreclose so many development and design options that it becomes hard to innovate a product that is both compliant and still has market potential.

In as far as regulation imposes constraints on some companies, however, it also creates a potential market opportunity for others, and thus a fourth possible response: innovating solutions to help companies achieve compliance without damaging their regular production and value-creation activities, that can be sold to those affected by the regulation in question. We call this fourth possible response *regulation-exploiting innovation*, since it exploits regulation as a market opportunity.[8] An example would be developing tools to anonymize data

[6] Comments by Johannes Caspar, head of the Hamburg Data Protection Authority, at the Competence Center for Applied Security Technology (CAST) Forum, 15 March 2018, Darmstadt, Germany

[7] It can be debated whether changing suppliers is best classified under the implicitly product design-focused concept of "compliance innovation" or whether it should be listed as a further, separate response (e.g. "organisational changes"). Here we have kept it under "compliance innovation", for two reasons. Firstly, we are concerned to preserve the framework's parsimony. Secondly, because the technical implementations of different vendors' offerings are likely to be not exactly identical, changing vendors is likely to require at least some own engineering work to ensure product functionality,

[8] Companies might also develop such tools purely to assist themselves with their own in-house compliance activities, without selling them to others.

so that analytics can be performed on it while remaining compliant with data protection law.

Whether companies recognize and try to exploit such innovation (and market) opportunities should again be determined by their technological and financial capability, how easy the innovation is expected to be, the degree of enforcement and the expected market demand for regulation-compliant products. Again, the onerousness of the regulation may also impact choices and outcomes: the more onerous it is, the harder it may prove to innovate solutions that truly help companies achieve compliance.

We focus on the level of enforcement and the level of expected market demand for regulation-compliant products for three reasons: Firstly, company-specific factors such as technological capability or financial resources are likely to vary randomly. Secondly, the easiness of different innovation options is difficult to predict ex ante and probably varies strongly across companies and applications. Thirdly, how onerous regulation *really* is, is likely to be driven by complex interactions of individual regulatory stipulations, technologies and business models, and is therefore likely to vary idiosyncratically across technologies and sectors, and should thus be hard to predict ex ante. The true onerousness level may only be established in the course of the entrepreneurial discovery process, as companies attempt innovation.

Generally, perceived high market potential for an innovation should stimulate efforts to innovate since firms try to exploit perceived opportunities, while perceived low potential ought to dampen innovation efforts. The same is true of enforcement: strict enforcement should create a strong need for solutions to achieve compliance, presumably stimulating innovation efforts, while lax enforcement would be expected to dampen this incentive. Taken together, the level of enforcement can be strict or lax, and the level of expected market demand for data protection regulation -compliant products can be high or low.

Importantly, while the level of enforcement is likely to influence the strength of demand for regulation-compliant products, other factors can drive market demand even absent significant enforcement. For example, compliance can have a signaling function, providing information about the general quality of a product. Customers may also value data protection for its own sake, or regard it as part of their value proposition. Therefore, customers may even demand products that offer *higher* levels of privacy and data protection than the minimal regulatory requirements (what we call "privacy-friendly products").

Based on these considerations, we derive a framework consisting of four hypothetical scenarios and their postulated effects on innovation (Fig. 1):

- *Scenario 1: strict enforcement of data protection regulation and high market demand for data protection regulation-compliant products.*

Strict enforcement and high demand for compliant products means there are few incentives to innovate non-compliant products, and strong incentives to innovate compliant products. Therefore we should expect to see little *strategic non-compliance*, high levels of *compliance innovation* and high levels of *regulation-exploiting innovation*. We also expect high levels of *abandonment*, since companies cannot always predict whether a product idea can be made compliant. In sum,

Market Demand for Data Protection Law-compliant Products

Regulatory Enforcement of Data Protection Law	**High**	**Low**
Strict	• *Strong disincentives to innovate non-compliant products & weak incentives for strategic non-compliance* • *Strong incentives for compliance and regulation-exploiting innovation*	• *Strong disincentives to innovate non-compliant products & weak incentives for strategic non-compliance* • *Weak incentives for compliance and regulation-exploiting innovation*
Lax	• *Strategic non-compliance possible but unclear incentives for innovating non-compliant products* • *Strong incentives for compliance and regulation-exploiting innovation*	• *Strategic non-compliance viable, few disincentives to innovating non-complaint products* • *Weak incentives for compliance and regulation-exploiting innovation*

Fig. 1 Conceptual Framework

data protection regulation is expected to simultaneously hinder and encourage innovation.

- *Scenario 2: strict enforcement and low market demand for data protection regulation-compliant products.*

This scenario also creates strong disincentives to innovate non-compliant products, but with fewer counter-balancing incentives for innovating compliant products. Therefore, we expect little *strategic non-compliance* (due to enforcement), little *compliance innovation* and little *regulation-exploiting innovation* (due to low demand for compliant products), but also high levels of *abandonment* (again due to enforcement). In this scenario, data protection regulation probably reduces overall levels of innovation.

- *Scenario 3: lax enforcement and high market demand for data protection regulation-compliant products.*

This scenario should simultaneously create strong incentives for compliance innovation and regulation-exploiting innovation (due to market demand) while also making *strategic non-compliance* viable. Provided there is market demand for both compliant and non-compliant products, we should see little *abandonment*. Under this condition (demand for compliant and non-compliant products) this scenario should see the highest overall levels of innovations.

- *Scenario 4: lax enforcement and low market demand for data protection regulation-compliant products.*

With lax enforcement, we should expect to see high levels of *strategic non-compliance* and low levels of *abandonment*. However, low demand for compliant products means we should also expect little *compliance innovation* and little *regulation-exploiting innovation*. In sum, in this scenario data protection regulation does not constrain innovation, but also does not encourage it, suggesting it should have little net effect overall. We use these concepts and scenarios to guide our empirical research.

4 Methodology

4.1 Data Collection and Analysis

For two reasons, we focus on German startups whose products or business models center on personal data. Firstly, Germany is likely to present a particularly affected business environment for companies that use personal data. Germany has had a leading role in the development of data protection law, and has deeply influenced the EU GDPR and DPD. Germany also has an established network of data protection authorities (DPAs), and spends more on them than any other EU country (Schütz 2018). Furthermore, the media and public opinion are quite sensitive to privacy issues. Secondly, startups are the firms often most likely to innovate new products and services (Hsu 2003); i.e., the effects of regulation on *innovation* are likely to manifest particularly clearly and quickly among startups. Startups are likely to have smaller budgets available for compliance than large or established firms, meaning that *negative* effects from regulation may also manifest particularly strongly among them. However, their greater flexibility and strong innovation-orientation means that startups may also be particularly likely to identify and exploit regulation-induced opportunities for innovations. These factors mean that any positive or negative effects data protection regulation may have on innovation are particularly likely to show up among German startups. Conversely, if privacy regulation has little effects on innovation among German startups, such effects are even less likely among other firms or in other countries.

Given the dearth of prior research and absence of strong, testable hypotheses, we chose an interview-based methodology as recommended by Myers 2009, to obtain a deeper understanding and develop and refine hypotheses about how data protection regulation may influence innovation among startups.

We divided the research into two stages. In the first, we interviewed 10 intermediaries involved in the startup ecosystem: 2 managers of university startup accelerators, 7 lawyers specialized in data-protection/IT law and startup clients, and 1 partner of a private VC fund. To triangulate our results, we also drew on a further 9 interviews: 6 with senior officials of German Data Protection Authorities (DPAs), and 3 with German corporate data protection officers. Each interviewee had a minimum of five years relevant working experience, and often significantly more. These interviews were conducted between March and August 2018. Building on the insights gained in the first round of interviews, we then interviewed 9 startups (the second stage of the research). These interviews were conducted in January and February 2019.

Table 1 Interviewed Intermediaries

Intermediary / Profession	City
Lawyer 1	Leipzig
Lawyer 2	Hamburg
Lawyer 3	Berlin
Lawyer 4	Berlin
Lawyer 5	Berlin
Lawyer 6	Berlin
Lawyer 7	Berlin
University Accelerator Manager 1	Berlin
University Accelerator Manager 2	Karlsruhe
VC Partner 1	Munich

The reason for first interviewing intermediaries was two-fold. Firstly, as they advise many startups in diverse sectors, we expected lawyers and consultants to be able to provide a broader overview than individual company executives, particularly concerning what kinds of innovation-obstructing or -stimulating effects data protection regulation commonly produced in startups, and how frequent and severe these effects tended to be. Given the work's exploratory nature and the relative lack of prior research, obtaining this broader overview seemed important in addition to help guide the following selection of startups for the second stage interviews. In particular, we sought information (primarily from the lawyers and DPAs) on the regulatory environment – how strict enforcement really was, what compliance strategies companies adopted, and which specific stipulations of data protection law tended to most obstruct (or stimulate) companies' innovation efforts. Secondly, given the intermediaries' long working experience, we expected them to able to describe both the pre-GDPR situation, and provide initial insights on how things are changing with the GDPR.

The interviewed intermediaries were identified through the main German startup magazine, *Gründerszene*, expert advice, and desk research. Among the 10 intermediaries, 6 were based in Berlin (Table 1). While this could introduce biases, we are not overly concerned about that as, firstly, Berlin's startup scene is itself very diverse, being Germany's most established startup cluster. Secondly, because most Berlin interviewees were lawyers who stressed that their clients came from across Germany.

The interviewed startups in the second stage were identified via university accelerators and desk research. We sought startups for which processing of personal data was at the heart of their products and business models, in particular companies where the processing was likely to pose a "high risk" with regards to the GDPR, as these companies could be expected to be particularly affected by data protection regulation.[9] As the interviews with the intermediaries indicated that data protection regulation's effects may vary depending on whether companies are situated in B2B or B2C markets, we sought to obtain a mix of both across different industries for the second stage. Eventually, 18 startups were contacted and 9 interviews secured. Tables 2 and 3 provide information about the sample composition. All but one of the startups were engaged primarily in "high risk" processing. The companies were between 2 and 14 years old (median: 5 years, average 6.7) and had between 5 and 50 employees. In most cases the interviewee was the company (co-)founder; in 3 cases it was the CTO, a senior product designer or the data protection officer, respectively. Of the interviewed founders, 3 doubled as CTO or otherwise led technology research and development, while 3 had primarily management responsibilities (though they mostly had engineering backgrounds). 4 companies were exclusively B2B companies; 5 served both B2C and B2B markets (usually by offering free products to B2C end-users and monetizing through paid-for B2B products). A wide range of industries were represented in the sample, including surveillance, personalized medicine, patient management, HR, assisted living, identity management and finance. Geographically, companies were drawn from Berlin, Karlsruhe, Frankfurt and Munich.

[9] Under the GDPR's "risk-based" approach, processing likely to pose a "high risk" to individuals faces higher regulatory scrutiny than less risky processing. While the GDPR provides no comprehensive definition of which operations are "high risk", the Article 29 Working Party of European DPAs has issued guidance identifying 10 processing operations where a "high risk" is likely, including processing of medical and financial data, data of vulnerable individuals (e.g. seniors, employees or job applicants), surveillance, and where processing can give rise to identity theft (Art. 29 WP 2017; see also Recital 75 GDPR).

4.2 Interview Structure

The interviews with both intermediaries and startups were conducted by telephone or on-site, taking ~45-90 min each, recorded, and transcribed. The interviews were semi-structured, i.e., the interviewees were asked a common set of questions but we also explored new topics as they brought them up in the conversation. Two basic questionnaires were used for the intermediary and startup interviewees respectively, adjusted to exploit presumed veins of expertise (e.g. lawyers were asked more fine-grained questions about the effects of specific data-protection law principles).

The interview guide for the intermediaries had four parts: Firstly, we asked interviewees about the types of firms they had as clients (sectors, business models, etc.). Parts 2 to 4 operationalized the conceptual framework outlined above: In particular, Part 2 prompted them to talk about challenges that startups in their experience encountered with data protection regulation (type, gravity and frequency of problems, etc.). Particular focus was given to whether, how and why data protection regulation may obstruct innovation, e.g. forcing product abandonment or redesign. Part 3 examined whether data protection regulation stimulates compliance innovation and/or regulation-exploiting innovation. We asked how companies respond to data protection regulation-related problems (e.g., with non-compliance, innovation of own solutions, purchase of solutions from third parties, other changes, etc.). We further asked respondents to assess the market potential for products and technologies using compliance or data protection-"friendliness" as a competitive differentiator. Part 4 turned to enforcement and asked after their experience and assessment of the strictness of data protection regulation enforcement. Finally, we asked respondents for a broad assessment of whether and why data protection regulation hinders or fosters innovation.

The interview guide for startups followed broadly the same structure. Respondents were first asked to describe

Table 2 Demographics of Interviewed Startups

Startup Number	Year Founded	Number of Employees	Interviewee Position	B2B or B2C	Industry
Startup 1	2008	8	Founder, R&D & managerial responsibilities	B2B	Facial Recognition, Machine Learning
Startup 2	2017	10	Founder, Head of R&D	B2C, B2B	Personalised Medical Care
Startup 3	2011	13	Founder, managerial responsibilities	B2B	Medical Patient and Care Managment
Startup 4	2015	50	Founder, CTO	B2C, B2B	HR, Job-Search and Job-Placement (2-sided Platform)
Startup 5	2014	8	Founder, managerial responsibilities	B2B, B2C	Finance, Identity Management, (Personal) Data Management
Startup 6	2005	50	Senior Product Designer	B2B, B2C	Company Builder for Digital Business Models
Startup 7	2014	8	Founder, managerial responsibilities	B2B	Ambient Assisted Living for Seniors
Startup 8	2009	9	Data Protection Officer	B2C, B2B	HR, Job-Search and Job-Placement (2-sided Platform)
Startup 9	2017	50	CTO	B2B, B2C	Identity Management & Authentication

their business model, products and customers. Then followed a series of questions about whether and if so, how, data protection regulation influenced their development of products, services and business model (positively or negatively) and what, if any, the main challenges were that data protection law created for them. Specific issues that the intermediary interviews had revealed to be possible constraints were explored (e.g. access to data, etc.). We probed them on how they dealt with data protection-related challenges (abandonment, redesign, innovating solutions, non-compliance, changes to legal contracts, etc.), how often challenges manifested, and how difficult they were to solve. To assess if markets for compliance and regulation-exploiting products were coming about in either the B2C and/or B2B sectors, we asked about how important, in their assessment, data protection compliance/"friendliness" was to customers and (end-) users, whether they purchased products or services (other than legal advice) to help them achieve compliance, and (more broadly) whether they saw markets developing for compliant products and products to help achieve compliance. In closing, we prompted them to make a broad assessment of whether and why data protection regulation hinders or fosters innovation.

The transcripts were first analyzed separately by the research team members to identify and interpret all interviewee statements relating to (1) our framework's explanatory variables (enforcement, market demand), (2) the possible company responses identified by our framework (abandonment, compliance innovation, non-compliance, regulation-exploiting innovation), and (3) any other statements relevant to our research questions, in particular any that challenged or departed from our framework (e.g. different company responses, other explanatory variables, …). Thereafter, we held a joint workshop for all four authors to discuss and establish agreement on how to interpret the statements with regard to the main variables of interest, and how to understand and conceptualize the company responses. We further triangulated the findings with the interviews with DPAs and DPOs (Data Protection Officers) and other primary and secondary documents.

Table 3 Geographical Distribution of Interviewed Startups

City	Number of interviewed Startups
Berlin	3
Karlsruhe	3
Frankfurt	2
Munich	1

5 Results and Discussion

5.1 Data Protection Regulation and Innovation Prior to the GDPR

The key finding from the first stage of interviews (with the intermediaries) was that contrary to common perceptions abroad, of data protection being particularly strict in Germany, in fact, prior to the GDPR, enforcement of data protection law had been quite *lax*. Non-compliance was a

viable, often-used corporate strategy to deal with data protection law. Partly due to this, demand for products compliant with data protection regulation was low, with some exceptions discussed below. Before the GDPR, there was thus only limited incentive to innovate regulation-compliant products.

All interviewed lawyers described enforcement in the pre-GDPR era as lax, and felt that startups in particular were largely ignored by the DPAs. The two university accelerator managers and the VC partner confirmed this in as far as they had never heard of enforcement actions against startups. This is borne out by the available data on fines levied by the DPAs for breaches of data protection regulation. For instance, from 2010 to 2017, in the federal states of Berlin, Bavaria and Hamburg, less than 20 enterprises were fined each year by their DPAs for data-protection law breaches. Average fines in Berlin came to less than €1800 (Bavaria: ~€3100; Hamburg: ~€10,000.[10]) (Martin et al. forthcoming).

Little systematic data on fines is available for the other federal states, but our interviews with lawyers and DPAs made clear that the picture elsewhere was substantively similar. The reasons for lax enforcement may partly be cultural (Bamberger & Mulligan 2013), but are certainly closely related to DPAs' hitherto limited personnel resources, which made enforcement difficult (Schütz 2018). Our DPA interviews also indicated that so far enforcement actions have mostly taken place when complaints from the public emanated, rather than due to proactive DPA investigations. This matters for startups, as complaints from the public have tended to focus on easily observed and understood data processing (above all video surveillance and direct mail advertising), not the kinds of technologically and organizationally complex processing (e.g. tracking-based online advertising) that technology startups are likely to deploy, but which lay people find hard to understand or attribute to their use of specific online services.

Lax enforcement shaped how startups responded to data protection law in the pre-GDPR period. Economists and criminologists argue that compliance is a function of the probability of detection multiplied with the expected severity of the sanction, if detected (Becker 1968, Faure et al. 2009). As we saw— at least prior to the GDPR— both were low, implying that compliance and thus demand for either compliance or regulation-exploiting innovations should have been low too. Our interviews largely bear this out, though they suggest that in some sectors compliance was important before the GDPR, too.

The interviewed lawyers consistently suggested that before the GDPR many companies operated in legal gray zones, what one may term "weak strategic non-compliance": trying to avoid egregious illegalities while engaging in practices of questionable legality whenever discovery risks seemed low and more unambiguously lawful alternatives costly. Several of the interviewed startup executives supported this view.

Companies could choose non-compliance as a strategy not only because enforcement was lax but because demand for regulation-compliant or "data-protection friendly" products was limited. On the B2C side, interviewees felt that, in practice most end users prized functionality and convenience over data protection, and lacked understanding of how privacy was invaded or protected. This limited the scope of data protection as a selling point. For example, Lawyer 1 described a social network that— in response to regulatory pressure and several scandals— had aggressively tried to brand itself as "privacy friendly", but found that users did not value this as a competitive differentiator, especially if it led to impaired functionalities.

On the B2B side, prior to the GDPR, things were more complex. Interviewees indicated that, at least until companies began giving serious thought to GDPR compliance in late 2017/early 2018, demand for products compliant with data protection law had been weak in most market segments. As Lawyer 4 put it, "[prior to the GDPR], there were many rules, but no one cared, because in practice they were not enforced." Incentives to innovate compliant products (or products to help others attain compliance) were thus limited. On the other hand, non-enforcement meant that data protection law also created few obstacles to innovation. While most interviewed lawyers knew of cases where products or business models in development had been abandoned due to data protection concerns or where VCs pulled back from planned investments, most considered these to have been very rare so far. Even blatantly illegal products and services continued to be developed by startups, if they were confident that discovery risks were low (Lawyers 2, 3, 4, 5, 6, 7).

However, in two B2B market segments compliance seems to have been more important, also prior to the GDPR. One of these was enterprise software and business IT/data systems, at least in as far as they were used to process data of employees, and the other was police and security services. VC Partner 1, University Accelerator Manager 2, Lawyer 5 and Startup Executive 1 all noted that complete data protection compliance was a basic prerequisite to work in these markets, putting real pressure on startups to innovate fully compliant products and services. In the case of police and security services this should not come as a surprise, since evidence obtained through non-compliant processing is likely to prove inadmissible in court. The case of software and data systems used to process employee data seems more surprising, but appears closely related to the position of the works councils in Germany. These are powerful players within firms, and German law grants them particular influence over the use of technologies to process employee data.

[10] The higher average in Hamburg is an artefact of two fines of €145,000 and €200,000 levied on Google and a local bank, respectively. The median fine was substantially lower the €10,000.

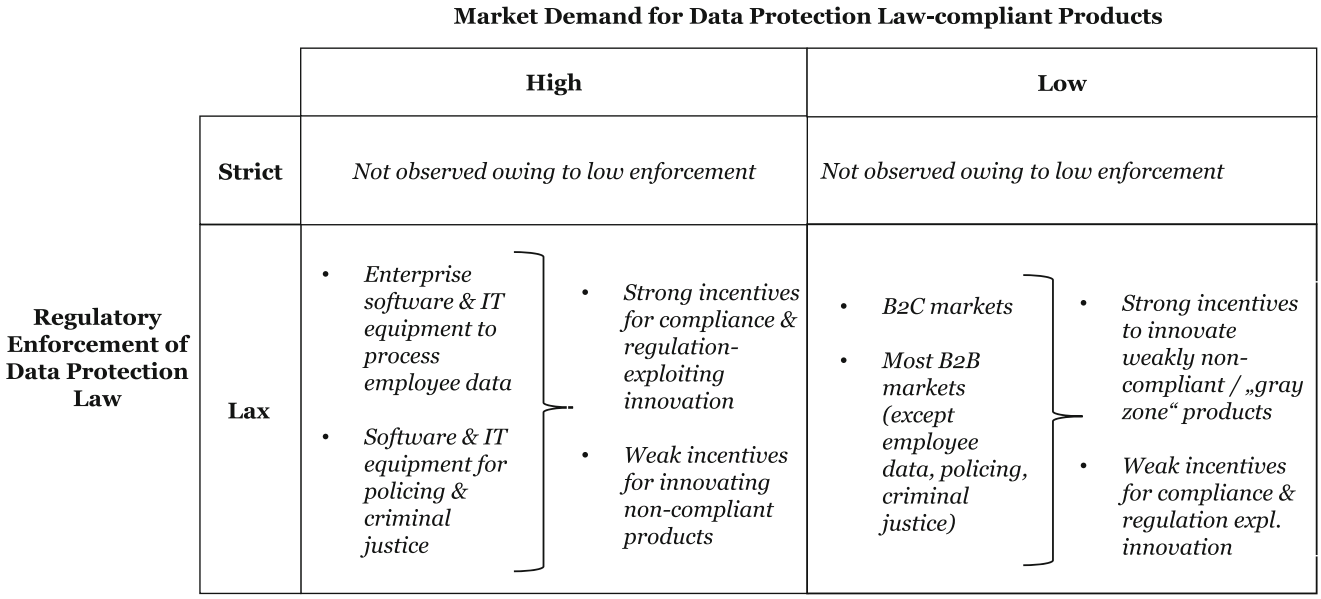

Fig. 2 Sectoral Effects of Data Protection Regulation prior to the GDPR

Returning to the hypothetical innovation outcomes mapped in Fig. 1, we can now map specific sectors to the quadrants (Fig. 2) for the pre-GDPR period. At least prior to the GDPR, the top quadrants were empty, due to lax enforcement. In the bottom right quadrant, we have the B2C sector, and much of the B2B sector. Lax enforcement and low market pressure (due to low end-user pressure) for fully data protection-compliant products and services limited data protection-related innovation in these sectors, at least before the GDPR. In the bottom left quadrant (lax enforcement/high demand) we have B2B companies supplying enterprise software and IT equipment used to process employee data, and for criminal-justice and policing work. High pressures for full data protection-compliance from work councils and the criminal justice system created market demand for suitable products, in turn incentivizing innovation.

5.2 Data Protection Regulation and Innovation under the GDPR

The second stage of interviews squarely indicated that with the advent of the GDPR, the enforcement environment and market demand have changed considerably, in turn altering the constraints on and the incentives for innovation that data protection law creates.

5.2.1 Changing Enforcement Environment and Market Demand

The interviewees and secondary evidence show that the enforcement environment is perceived to have become a lot tougher with the GDPR. Startup Executive 4, for example, volunteered that in his understanding, the DPAs were now switching from "advisory mode" into "prosecution mode". This preoccupied him "day and night". Other executives used less drastic language, but also consistently indicated that enforcement was perceived to have become significantly tougher and that much greater attention was now given to compliance than before (Startups 2, 3, 5, 6, 8). This is consistent with the evidence from the interviewed lawyers, DPAs and DPOs, and the broader media coverage surrounding GDPR implementation in Germany. Consistently, they suggest that companies across the economy devoted substantial resources in 2018 to achieve basic compliance with data protection law, often for the first time.[11]

The main driver of this development seem to have been the new fining powers of the DPAs. Under the old Federal Data Protection Law the maximum fine for violations was €300,000. The GDPR increases this maximum fine to €20 Million or 4% of annual worldwide turnover – whichever is greater. Interviewed DPAs indicated that they felt under considerable political pressure to make use of these new powers and step up enforcement. To do so, the German DPAs have received budget and staff increases, at least somewhat mitigating the previously dramatic imbalance between resources and tasks that hitherto had hampered enforcement. While this imbalance remains to some extent, DPAs have argued that the GDPR allows them to compensate for this by imposing particularly severe fines, in order to act as

[11] The GDPR creates some new rules, but many of its requirements are not new and have been mandatory under German data protection law for decades. The dash to achieve GDPR compliance was often a catch-up operation whereby measures that the law had for many years required were finally implemented. (Startup Executive 8; Interview, corporate Data Protection Officer, 13 March 2018).

a deterrence.[12] The GDPR has also strengthened people's rights to lodge complaints with DPAs, and of NGOs and other third parties to take companies to court over illegal data-processing practices. People seem to be using these new rights fairly frequently: Since May 25, 2018, the number of complaints about (supposedly) illegal data processing lodged with DPAs has doubled or even quadrupled (Martin et al. forthcoming). Companies also face the risk that if they fail to adhere to the law, competitors may denounce them to the authorities, a concern Startup Executive 4 stressed.

How tough an enforcement environment will really develop in the medium term remains to be seen. For the moment though, it seems clear that companies perceive enforcement to have become substantially stricter. Since perceptions are what ultimately matters for setting incentives, we therefore argue that under the GDPR most sectors should now be located in the upper quadrants of Fig. 1: high enforcement.

The new enforcement environment is reshaping market demand. The interviewed executives consistently stated that nowadays complete compliance – or at least a credible claim thereto – was a necessary condition to play in B2B markets. As Startup Executive 4 put it, "[to play in the B2B space] in Germany or Europe, you must advertise that you are GDPR-compliant, otherwise you can forget it". This is not to say that complete compliance is being universally achieved. One startup executive (interview number withheld) argued that the GDPR's many documentation requirements meant that for firms with high turnover among users and rapid releases of new products, staying on top of *all* compliance requirements *all* the time was almost impossible.[13] Everyone claimed to be fully compliant, but in his view, this was partly "window dressing". Several other interviewed executives entertained similar doubts, but also made clear that compliance had now become a key criterion for selecting suppliers and business partners. Several had discontinued business relations due to doubts about the counter-party's compliance level.

In short, in B2B markets the demand structure today is very different to the one interviewees described for the pre-GDPR period. Strategic non-compliance is no longer seen as a viable strategy, it is felt necessary to avoid non-compliance at all costs, and business relations can hinge on providing credible compliance assurances. Hence, for B2B markets we see demand for regulation-compliant products as "high".

In B2C markets, the picture is somewhat different. Much like the interviewed intermediaries, most startup executives felt that for most end users functionality continued to come first and that most lacked understanding of data protection issues (Startup Executives 2, 3, 4, 5). They believed that "data protection friendly" had only limited potential as a competitive differentiator, since ultimately most users chose products on grounds of functionality and price. However, Startup Executives 6 and 8 noted that users were becoming increasingly aware of data protection issues – though they often remained confused – and suspicious of corporate efforts to collect data. Startup 6 was therefore increasingly careful and restrictive in its data-collection practices, to avoid frightening off users. Similarly, Startup 9 had discontinued – legal – tracking practices, because it felt "spying" on users in this fashion was inconsistent with its value proposition as a trusted intermediary. Startup 1 had also abandoned a product idea (customer analysis for brick-and-mortar retailers based on facial analysis), because its intended customers (the retailers) thought their end customers would feel this was too privacy-invasive. On balance, we therefore see *end user* demand for data protection compliant or "friendly" products as neither high nor low, but moderate.

We thus find ourselves approximately in the first of the scenarios mapped out in Section 3; *strict enforcement* and *moderate to high market demand for regulation-compliant products*. We postulated that in this scenario, regulation should have both significant innovation-stimulating and -constraining effects. Encouraging, because market demand and enforcement pressures should incentivize compliance innovation and regulation-exploiting innovation. Obstructing, because these same forces render strategic non-compliance unviable, obliging firms to abandon products or ideas that cannot be made compliant.

Consistent with this theoretical prediction, our interviews provide evidence for both innovation-encouraging and -obstructing effects. Net effects (more or less innovation in total) relative to a hypothetical no-regulation baseline are hard, maybe impossible, to determine. Arguably more important is the evidence that our interviews provide that innovation-obstructing effects seem to be disproportionately affecting specific technologies and business models. The next sections lay out the evidence and discuss policy implications.

5.2.2 Innovation-Stimulating Effects of Data Protection Regulation

Our theoretical framework identified two innovation-stimulating responses that data protection regulation might trigger in firms: firstly, by prompting companies whose products or ideas are directly affected by the regulation to respond by engaging in *compliance innovation* to make their products/ideas compliant with the regulation. Secondly, by prompting companies to respond with *regulation-exploiting innovation*, to innovate products that will assist companies affected by the regulation in achieving compliance. As laid out below, based on our interviews we obtained little evidence for compliance

[12] Comments by Johannes Caspar, head of the Hamburg Data Protection Authority, at the Competence Center for Applied Security Technology (CAST) Forum, 15 March 2018, Darmstadt, Germany.

[13] Two other startup founders felt this attitude was unjustified "moaning" since "the requirements aren't that onerous".

innovation, but clear evidence for regulation-exploiting innovation. We also found evidence for a further response: *buy European*.

Compliance Innovation None of the interviewed startups had *themselves* undertaken significant innovations in response to the regulation. Where needed, technological solutions were instead sourced on the market. As Startup Executive 2 explained, innovating their own core products was ample work; innovating additional data-protection technologies outside of their own core competencies was out of the question. However, Lawyer 3 recounted two cases of startup clients who had developed innovative de-identification/anonymization technologies to be able to provide their own customers with regulation-compliant analytics services, suggesting that compliance innovation does occur.

Regulation-Exploiting Innovation Conversely, there is clear evidence for the GDPR sparking a market for "regulation-exploiting" technologies to support data protection and compliance. Six of the nine interviewed startups had introduced new third-party technology or purchased technology services to this end, including data protection compliance management software (to help monitor and document user consent, use of tracking software, and generate compliance documentation), and IT security products and components (e.g. password managers, encryption libraries). One startup had hired IT security experts to conduct penetration tests and certify their security measures. This is consistent with findings from a representative survey of German small and medium-sized firms, which found that the GDPR had promoted some 50% of respondents to increase their IT-security measures (GDV 2019). More broadly, there are indications that the GDPR's stricter rules about reporting data breaches, in particular, has led companies to improve IT security, sometimes coming from a very low base line. For instance, Lawyer 2 recounted the example of a law firm that had been prompted to migrate its client (!) data from an unsecured, open cloud to a secure, private commercial cloud.

Lawyers 5, 6 and 7 and Startup 3, 6 and 9 described a lively and innovative market developing for products to enable companies achieve compliance and solve obstacles from data protection regulation. Startups 5 and 9 had themselves entered this market to exploit opportunities created by the GDPR. They were developing identity, consent and data-management products to help businesses handle, verify and document user identities, data streams and consent across platforms, and increase users' control over their data.

Development of a growing GDPR-driven market for data protection-related products is indicated also by the data compiled in the International Association of Privacy Professionals (IAPP) Privacy Tech Vendors Reports. The IAPP defines "privacy technology" as "technological solutions for organizations working towards data protection accountability, compliance and [data protection] risk-assessment and -mitigation." (IAPP 2017, p. 6). The 2017 Report listed 51 vendors across 9 product categories, while the 2018 report identifies 192 vendors across 10 product categories (IAPP 2018). Almost 40% of these companies had been founded in the last five years, with 48% being headquartered in Europe.

Further Effect "Buy European" Evidence also emerged of the GDPR sparking a "buy European" effect as companies seem to be becoming wary of using non-European providers of digital services (e.g. cloud storage), both for fear of falling foul of data protection law, and as a simple way to make compliance easier. Startups 2 and 7 noted that they categorically refrained from using non-EU digital-service providers, at least for all important functions, as they believed that data protection could not otherwise be guaranteed. Startup 4 had taken no final decision, but was edging towards this view, too. Startups 5 and 6 stated that while they remained open to using non-EU providers in principle, in practice however, they often preferred using European or even German providers, if only "to feel a little safer" and because being located in the EU served as a signaling mechanism: it was "implicitly assumed" that they "would have fully implemented the GDPR", in turn reducing worry and workload, because there would be less need to check all details.

It is important to be clear about what innovation-related effects such regulation-induced preferential purchase of European companies' products may and may not have. In the first instance, it only expands the market for local relative to foreign producers, and creates incentives for European companies to replicate services offered by non-EU firms. It does not directly create incentives to innovate radically new or improved products. In the medium term, though, it may lead to genuine increases in innovation, if it promotes growth in the overall number of service providers and intensified competition among them.

5.2.3 Innovation-Constraining Effects of Data Protection Regulation

The main potential negative, innovation-constraining response that our theoretical framework identified was *product abandonment*, that data protection regulation might prompt firms to respond by *abandoning* products or product ideas that were judged fundamentally incompatible with the regulation. Our interviews found evidence for abandonment and also identified two further innovation-constraining responses: *entrepreneurial discouragement*, whereby concerns that data protection law will make realization of their ideas impossible might discourage would-be founders from starting firms, and what we label "*data minimization*", whereby the cumulative impact of privacy regulation reduces innovators' access to data to such an extent that certain products and technologies,

especially in the field of big data and artificial intelligence, become hard to develop for lack of input data.

Entrepreneurial Discouragement With regard to *entrepreneurial discouragement* the interviewees' pronouncements varied. University Accelerator Manager 2, Lawyers 2 and 4, and the founder of Startup 4 considered it a serious concern. Startup 4's founder went as far as to say that he would not found his company again today, given the constraints created by the GDPR. Most other executives though doubted that data protection law would discourage many entrepreneurs. Founder 3 was even openly dismissive ("that would be a bad entrepreneur ... I would not advise such a person to start a company").

Product Abandonment Four of the interviewed startups (Startups 1, 4, 6 and 7) had abandoned planned or already implemented products, services or features due to data protection concerns. While Startup 6 stressed that the abandonments had concerned only a few minor things that were not important value drivers, Startup 4 placed the number of abandonments at 20% of all more seriously pursued product ideas. Interestingly, it referenced compliance costs as a perhaps greater driver of abandonment than legal restrictions per se. While some ideas had been abandoned because it was thought impossible to implement them in ways that would be both legal and effective (e.g. because of doubts that users would consent), more were abandoned because compliant implementation (and determining if and how the idea might be made compliant at all) was too expensive. With Startup 7, abandonments were more occasional (though they concerned valuable features, like voice and light recognition) and were driven by concerns that offering these features at the required quality level would require using non-European service providers. Startup 1 presents a different case: it too had given up on one product idea due to privacy concerns (visual recognition-based analysis of brick-and-mortar retailers' end customers), but not for reasons of law: it would have been legal, but the retailers' felt the system would violate their customers' privacy preferences.

All the interviewed lawyers had experienced cases where, legally, clients would have been obliged to abandon products or features in order to maintain compliance, but their estimates of the frequency of such cases diverged considerably. We asked lawyers to estimate in what percentage of cases where they had advised startups on data protection law issues, products would properly have had to be abandoned to ensure compliance, because legal operation would have been impossible. While Lawyers 1, 5, 6 and 7 placed these cases in the low single-digit percent, Lawyers 2 and 3 gave figures of 15 and even 30%. (Lawyer 4 refused to venture a figure.) It is unclear how often the lawyers' evaluations actually led to abandonment: as noted, pre-GDPR, firms often preferred to run the legal risks rather than forego promising ventures.

These numbers must be treated with caution, as indicative at best. For one, while we asked the lawyers about their sectoral specializations, we know little about the underlying case populations from which the different estimates were drawn. In addition, the ease with which a given data-protection law problem can be solved can vary considerably by company and across time: a problem that one firm can easily solve – because it has the necessary financial resources, or the brand reach and strength of offerings to induce end users to give consents – another company may be unable to solve, leaving it only the choice of abandonment or illegality. Similarly, a problem that may be impossible to solve retrospectively without seriously damaging the business (e.g. retroactively collecting consents from users long signed up for a particular feature) may be very easy to solve prospectively (asking new users to consent).

While the range of (serious) problems with data protection law that companies encounter are most likely diverse, the interviews with Lawyer 1, 4, 5, 6 and 7 and Startups 1, 2, 5, 6 and 9 indicated that problems seem to be most severe and appear most systematically in data-driven business models that share either one or two structural features: *lack of a direct relationship to the end users ("data subjects")* and/or *inability to offer the "data subjects" direct and tangible benefits from the processing*. The interviewees also suggested that big data analytics, artificial intelligence and parts of the digital consumer economy (e.g. location-based services) may be particularly affected by the constraints on companies with these structural features.

The difficulties business models marked by these features encounter is driven by two core principles of European data protection law: firstly, the need for data processing to have a legal basis, and secondly the purpose-limitation principle. Data protection law stipulates that processing is only permitted if it has a legal basis. The GDPR, the previous DPD and the national laws define six legal bases, of which three are most relevant here: processing is legal if the "data subject" (the person whose data is to be processed) has consented, if it is necessary to perform a contract between controller and data subject, or if processing is necessary for purposes of the legitimate interests of the data controller, unless these are overridden by the rights and interests of the data subject. Under the purpose-limitation principle, the purposes of the processing must be specified in advance. Further processing for new purposes that have no relation to the original purpose is illegal, unless a new legal basis is obtained for the new processing (e.g. a new consent).[14] The next paragraphs elaborate how these legal stipulations become problematic for companies.

[14] Further processing for scientific, statistical or historical purposes is excepted from this rule.

Lack of a Direct Relationship to End Users/Data Subjects Examples mentioned by interviewees include third-party providers of services like auto or sports insurance as well as location-based recommendations, who, lacking a direct relation, must access users via second-party platforms that *have* such relationships (e.g. the companies providing users' cars or smartphones). This leaves providers dependent on said platforms to obtain the necessary legal bases for processing (e.g. users' consent to the platform passing on their data). Another example repeatedly mentioned are firms (and university researchers) active in artificial intelligence or big data who depend on third parties that have the requisite relations to data subjects (e.g. hospitals, public administrations, B2C companies) to provide them with data and legal bases. The purpose-limitation principle creates additional barriers in this context, as it makes it harder to repurpose or share data sets.

Inability to Offer Users/Data Subjects Direct and Tangible Benefits from the Processing The GDPR sets higher standards for what counts as valid consent than previous data protection law. Organizations cannot ask for blanket consent to any and all processing they might sometime want to perform, cannot make provision of services dependent on consent to unrelated processing (i.e., cannot ask data subjects to "pay" with their data), must provide data subjects with easily understandable information about the planned processing, and cannot treat users' failure to opt out of pre-set settings as implying consent. This makes obtaining consent for processing that do not provide direct, tangible benefits to data subjects difficult even for companies that *have* direct relationships with end users, because users are less likely to consent to processing that offers them little in return, or bother to opt in to settings they are opted-out of by default.[15]

The problems arising in these constellations are not unsolvable per se. However, current proven legal, technological and organizational solutions and infrastructures to allow actors in complex data-processing chains to obtain legal bases and exchange data in ways that are simple and inexpensive for organizations and entrepreneurs, and seamless and uncomplicated for the users, are still lacking. This introduces sufficient friction as to, in some situations, block access to data and thus to innovation. As later discussed in Section 6, this is not exclusively a bad thing. Not all innovations are desirable for users or society. However, clearly there is risk of inadvertently blocking the development of desirable products and technologies.

[15] "Legitimate interests" provide an alternative legal basis, but the balancing this requires between the company's interests and those of the data subject leave this an uncertain foundation to build a business model on. As Lawyer 5 observed, the absence of case law combined with data protection law's vagueness means there is no guarantee that courts and DPAs may not come to a very different assessment of the balance struck than the company did.

Data Minimization The interviews commonly suggest that startups are adopting technology development processes that pays much more attention to data protection and privacy in general, and significantly closer to the privacy by design approach than was common hitherto (Waldman 2018). One aspect of this is that they seem to be taking a much more deliberate and self-restrictive approach to data collection, trying to minimize the collection to those data points that are really needed for a given purpose. Thus Startups 4, 5, 6 and 9 spoke of trying to avoid collecting data on a "nice to know"-basis without clear need or justification. Lawyer 5 similarly noted that she and her colleagues discouraged collection of data for which there was no clear need.

This choice, to limit collection only to clearly necessary data points, was motivated partly by concern over remaining compliant with the law, and partly by perceptions of user expectations and companies' own value propositions. As noted above, Startup 9 had discontinued user tracking, because it felt that such "spying" was inconsistent with the trust relationship it sought to build. Startup 6's executive similarly argued that users were becoming more suspicious of data collection and more prone to break off service usage/registration if they felt data collection was excessive. It is at present not possible to state what the longer-term effects on innovation of this apparent trend towards reduced data collection will be. While positive from the perspectives of privacy and data security, less data may also make it harder for companies to optimize products (a problem noted by executive 6) and innovate new ones. More broadly, the constraints on data sharing discussed above that result from the need for a legal basis and the purpose-limitation principle can hamper innovators' access to data. Startup 1, which depends on access to substantial and diverse volumes of human facial and bodily images, described this as a serious problem. While it had never been obliged to abandon *products* (or product ideas), limited access to data constrained its abilities to develop new things. There is thus the danger that data protection regulation will lead to companies being in effect "starved" of data. This could have particularly negative impacts on innovation in data-intensive fields like artificial intelligence.

6 Implications

Our interviews reveal data protection law to have both innovation-stimulating, and innovation obstructing effects and suggest that both have only become pronounced once the GDPR changed the enforcement environment and market demand for compliant products and processes. This finding, that hitherto data protection law simply had not had much effect because it had gone unenforced, has important implications for debates about the causes of the relative weakness of the European digital economy: at least for startup innovation in

the pre-GDPR era, data protection law would *not* seem to have been a significant cause.

The second implication of our findings is that the GDPR seems to be achieving some of its intended effects: As the Cambridge Analytica scandal underscores, data-based innovation is not always positive. The GDPR was created to protect people more effectively from processing that threatens their rights and interests. A certain volume of products or ideas being abandoned or substantially changed is thus what we should expect if the regulation is effective. The question of course is whether only "bad" innovations are being obstructed, or whether also "good" innovations are ending up as collateral damage of the regulation. Based on our results, it is notable that most of the product abandonments described to us in detail involved data processing which might indeed be considered socially problematic: Should a startup that plans to process large volumes of sensitive financial data, which is connected to named individuals and companies, really be in business if it cannot adequately secure the data? Should a company "enrich" job applications with background information and analytics on the job seekers culled from their social-media accounts and online presences?

Yet our interviews also indicate that data protection law in its current form may obstruct a broader range of data-driven business models and innovations than just "bad" ones, namely all those that lack direct relations to data subjects or are unable to offer them direct benefits from the processing. Big data and artificial intelligence may be particularly impacted by this. This would hardly be desirable. Given the significance these technologies hold for further scientific and economic advance (Legner et al. 2017), policy makers as well as researchers would be well-advised to carefully monitor developments in this space and support the development of appropriate solutions, such as de-identification/anonymization technologies and better consent-management and data-sharing infrastructures. They may also explore how the legal flexibilities built into the GDPR, such as the risk-based approach, legitimate interests, and exceptions for processing for "statistical" purposes may be used to create legal space for big data and artificial intelligence to flourish. Yet it is important not to exaggerate the constraints caused by data protection law. Only two of the interviewed startups regarded it as seriously constraining their activities. For all others it was at most a minor constraint, and often not even that.

The interviews further indicated that, as theory would predict, the GDPR has sparked considerable effort to develop "regulation-exploiting" innovations, i.e., efforts to turn regulation into an entrepreneurial opportunity by innovating solutions to the regulatory challenges created. These innovation efforts seem to mostly still be young and it still needs to be seen how effective the innovated solutions to the compliance challenges posed by data protection law really will be.

There is also the question of longer-term dynamic effects arising from regulation. As discussed above, the GDPR seems to have unleashed a certain "buy-European" response that may, over the medium term, lead to more innovation if it prompts more entrance and stronger competition in digital markets. It also seems to have sparked greater uptake of IT security measures across enterprises, which may pay substantial dividends in terms of reduced damages arising from data breaches.

7 Conclusion and Limitations

Use of personal data is increasingly important to companies, but its collection and use is affected by data protection regulation to safeguard people's privacy. Despite frequent company complaints about regulatory burdens, little was known about data protection regulation's actual effects on particular corporate functions. What was also lacking were investigations into companies' concrete responses to data protection regulation.

We helped fill this gap with our study on startup innovation. We revealed that the regulation did not have a single, overarching positive or negative effect, but rather a variety of partly countervailing effects, driven by the way specific stipulations and principles in the regulation interacted with the structural features of particular business models. We identified six concrete firm responses to data protection regulation. Three of these tend to have positive, innovation-stimulating effects: compliance innovation, regulation-exploiting innovation, and "buying European". In contrast, three other responses have more negative, innovation-constraining effects: abandonment, entrepreneurial discouragement, and data minimization. Overall, the regulation clearly stimulated a certain amount of innovation and market opportunities, but it also appears to obstruct certain business models and technologies, in ways that policy makers probably did not intend. We provided a framework to help make sense of these countervailing effects, and elucidate the mechanisms underlying them. Our work underscores the need for researchers to dig deep into the individual stipulations of regulation and how these interacts with specific business models and technologies, and to pay close attention to whether regulation is in fact enforced, rather than taking that as given.

Naturally, our study has limitations. Firstly, our theoretical framework and research focus primarily concerned how regulation affects product innovation and strategy. But companies can also respond to regulatory challenges by making organizational or purely legal-formal changes, to remove themselves from the purview of the regulation instead of implementing any substantive changes to the product itself. Examples include moving to a different jurisdiction (forum-shopping), or changing the legal bases of their activities (e.g. from consent

to fulfillment of contract, in the case of data processing). While moving abroad is unlikely to be an option for many startups, making more purely legal changes may sometimes be possible. It would be desirable for future research to further explore how common this is as an alternative response, and how companies (and lawyers) choose between these different options.

Second, owing to the rather small sample size we did not strive for representativeness. Instead, we carefully selected both intermediaries and startups to represent a wide range of stakeholders, business models and sectors. We ensured that all interviewees had substantial relevant experience, and chose startups that were particularly likely to be affected by data protection regulation – i.e. those, where data protection regulation's effects on innovation were likely to manifest most clearly. Future work should seek to validate (or falsify) and further specify the representativeness of the exploratory findings presented here, especially through large-scale quantitative work. Of particular interest is whether our findings – which derived from studying a sample restricted to data-driven startups in Germany – translate to other firm types and business models, such as more established and/or lower-tech SMEs and large corporations, or business models where data is less important. It is also of high interest to quantify potential differences across sectors (e.g. automobile vs. medical technology), and to assess the generalizability of the findings for other countries. Germany pays comparatively high attention to privacy, yet privacy concerns are influenced by cultural factors and vary substantially across countries (Reay et al. 2013). Even how the GDPR is interpreted and enforced differs to some extent across Europe. It is thus possible that its effects on innovation vary.

A further limitation derives from our selection of interviewees. We mainly spoke to C-suite executives (company founders, CTOs) and intermediaries (especially lawyers), and also drew on separate interviews with regulators. This approach seemed justified by our interest in how regulation impacts businesses' strategic decisions over product innovation – decisions which are often taken at the C-level (e.g. abandoning product lines, developing new regulation-exploiting products, etc.). However, at the more operational level regulation may also shape engineers' "smaller", everyday choices over product design, that collectively can have important consequences. Indeed, we glimpse just this in our interviewees' statements about trying to minimize the amount of data collected. In our case, due to the rather small size of the interviewed companies, the potential gap in perspective between founders and CTOs concerned with innovation/product strategy and lower-level engineers' focus on practical design questions was, in our case, probably fairly small. However, future research should more systematically explore how the GDPR is (re-) shaping engineers' everyday design choices.

Interviewee bias is also a potential concern. While interviewees might not have honestly stated all the facts, we did assure all interviewees of anonymity. Moreover, interviewees repeatedly made controversial or even potentially self-incriminating statements, or endorsed positions that did not obviously correspond to their narrow material interests. We always pushed interviewees to back up their opinions with facts from their direct experience, to help us evaluate their views. Therefore, we are not overly concerned over the potential for our results to be distorted by selective omissions or strong ideological beliefs. Of greater concern is the potential for inadvertent biases due to interviewees' own limited perspectives, as alluded to in the previous paragraph. Thus we recommend that future research should pay particular attention to the perspective and choices of engineers and designers below the C-level.

Timing may have also influenced our results. We conducted our interviews when the GDPR had just come into force. Respondent answers might thus have been excessively colored by initial, short-term compliance costs, and given insufficient attention to the possible longer term effects. This matters because empirical research has repeatedly suggested that especially positive effects of regulation tend to only manifest over the longer term. We therefore recommend that researchers continue to explore this topic over the longer term.

Acknowledgements A previous research in progress version of this manuscript was presented at the 2018 International Conference on Information Systems (Martin & Matt 2018). We are very grateful for the constructive feedback we received from conference participants as well as from the special issue editors and the entire review team. Funding for this research was kindly provided by the German Federal Ministry of Education and Research as part of the interdisciplinary research project "Privacy Forum" (www.forum-privatheit.de) for Nicholas Martin and Christian Matt, by the DFG Graduate School 'Innovation Society Today' for Crispin Niebel and by the European Union's Horizon 2020 research and innovation programme Grant Agreement No. 778420-EURITO for Knut Blind.

References

Albashrawi, M. & Motiwalla, L. (forthcoming). Privacy and personalization in continued usage intention of mobile banking: An integrative perspective. *Information Systems Frontiers*, 1-13.

Ambec, S., Cohen, M. A., Elgie, S., & Lanoie, P. (2013). The porter hypothesis at 20: Can environmental regulation enhance innovation

and competitiveness? *Review of Environmental Economics and Policy, 7*(1), 2–22.

Article 29 Data Protection Working Party (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. Accessed 27 February 2019.

Baesens, B., Bapna, R., Marsden, J. R., Vanthienen, J., & Zhao, J. L. (2016). Transformational issues of big data and analytics in networked business. *MIS Quarterly, 40*(4), 807–818.

Bamberger, K. A., & Mulligan, D. K. (2013). Privacy in Europe: Initial data on governance choices and corporate practices. *George Washington Law Review, 81*(5), 1529–1664.

Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169–217.

Blind, K. (2012). The influence of regulations on innovation: A quantitative assessment for OECD countries. *Research Policy, 41*(2), 391–400.

Blind, K. (2016). The impact of regulation on innovation. In J. Edler, P. Cunningham, A. Gök, & P. Shapira (Eds.), *Handbook of innovation policy impact* (pp. 450–482). London: Edward Elgar Publishing.

Blind, K., Bührlen, B., Menrad, K., Hafner, S., Walz, R., & Kotz, C. (2004). New products and services: Analysis of regulations shaping new markets. Fraunhofer Institute for Systems and Innovation Research, Karlsruhe. http://publica.fraunhofer.de/documents/N-24301.html. Accessed 26 February 2019.

Blind, K., Petersen, S. S., & Riillo, C. A. (2017). The impact of standards and regulation on innovation in uncertain markets. *Research Policy, 46*(1), 249–264.

Bourke, J., & Roper, S. (2017). Innovation, quality management and learning: Short-term and longer-term effects. *Research Policy, 46*(8), 1505–1518.

Campbell, J., Goldfarb, A., & Tucker, C. (2015). Privacy regulation and market structure. *Journal of Economics & Management Strategy, 24*(1), 47–73.

Carpenter, D., McLeod, A., Hicks, C., & Maasberg, M. (2018). Privacy and biometrics: An empirical examination of employee concerns. *Information Systems Frontiers, 20*(1), 91–110.

Cho, H., Rivera-Sánchez, M., & Lim, S. S. (2009). A multinational study on online privacy: Global concerns and local responses. *New Media & Society, 11*(3), 395–416.

Christensen, L., Colciago, A., Etro, F., & Rafert, G. (2013). The Impact of the Data Protection Regulation in the EU. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.657.138&rep=rep1&type=pdf. Accessed 26 February 2019.

Clemons, E. K., & Banattar, J. (2018). Regulating online privacy: Some policy guidelines, including guidelines for international harmonization. *Proceedings of the 51st Hawaii International Conference on System Sciences*, Big Island, HI, USA

Clemons, E. K., & Madhani, N. (2010). Regulation of digital businesses with natural monopolies or third-party payment business models: Antitrust lessons from the analysis of google. *Journal of Management Information Systems, 27*(3), 43–80.

De Hert, P., & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. In E. Claes, A. Duff, & S. Gutwirth (Eds.), *Privacy and the criminal law* (pp. 61–104). Intersentia: Antwerp and Oxford.

Deloitte. (2013). Economic impact assessment of the proposed European General Data Protection Regulation. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-european-data-protection-tmt.pdf. Accessed 26 February 2019.

D'Este, P., Immarino, S., Savona, M., & von Tunzelman, N. (2012). What hampers innovation? Revealed barriers versus deterring barriers. *Research Policy, 41*, 482–488.

Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., & Colautti, C. (2006). Privacy calculus model in e-commerce – A study of Italy and the United States. *European Journal of Information Systems, 15*(4), 389–402.

Economist. (2018). America should borrow from Europe's data-privacy law. https://www.economist.com/news/leaders/21739961-gdprs-premise-consumers-should-be-charge-their-own-personal-data-right. Accessed 26 February 2019.

Enzmann, M., & Schneider, M. (2005). Improving customer retention in e-commerce through a secure and privacy-enhanced loyalty system. *Information Systems Frontiers, 7*(4-5), 359–370.

Faure, M., Ogus, A., & Philipsen, N. (2009). Curbing consumer financial losses: The economics of regulatory enforcement. *Law & Policy, 31*(2), 161–191.

GDV Die Deutschen Versicherer (2019). Cyberrisiken im Mittelstand. Ergebnisse einer Forsa-Befragung Frühjahr 2019. https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberrisiken-im-mittelstand-2019-pdf-data.pdf Accessed 16 September 2019.

Goldfarb, A., & Tucker, C. E. (2011). Privacy regulation and online advertising. *Management Science, 57*(1), 57–71.

Hallinan, D. 2018. Feeding Biobanks with Genetic Data: What role can the General Data Protection Regulation play in the protection of genetic privacy in research biobanking in the European Union? Brussels: Vrije Universiteit Brussel PhD Thesis.

Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2016). Capturing value from big data–a taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management, 36*(10), 1382–1406.

Hildebrandt, C., & Arnold, R. (2017). Economic Impact of the ePrivacy Regulation on Online Advertising and Ad-based Digital Business Models. Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste. https://www.wik.org/fileadmin/Studien/2017/WIK_ePrivacy_study_ENGLISH.PDF. Accessed 26 February 2019.

Hsu, S. (2003). Internet privacy and security: A startup's perspective information dynamics in the networked society. *Information Systems Frontiers, 5*(1), 9–13.

IAPP (2017). 2017 Privacy Tech Vendor Report. The International Association of Privacy Professionals.https://iapp.org/media/pdf/resource_center/Tech-Vendor-Directory-1.4.1-electronic.pdf. Accessed 26 February 2019.

IAPP (2018). 2018 Privacy Tech Vendor Report. The International Association of Privacy Professionals. https://iapp.org/media/pdf/resource_center/2018-Privacy-Tech-Vendor-Report.pdf. Accessed 26 February 2019.

Khansa, L. & Liginlal, D. (2007). The influence of regulations on innovation in information security. *Proceedings of the 13th Americas Conference on Information Systems*, AMCIS 2007, Keystone, CO, USA

Kim, J., Baskerville, R. L., & Ding, Y. (forthcoming). Breaking the privacy kill chain: Protecting individual and group privacy online. *Information Systems Frontiers*, 1-15.

Koźluk, T. & Zipperer, V. (2014). Environmental policies and productivity growth: A critical review of empirical findings. *OECD Journal: Economic Studies. 2014*(1), 155-185

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., & Ahlemann, F. (2017). Digitalization: Opportunity and challenge for the business and information systems engineering community. *Business & Information Systems Engineering, 59*(4), 301–308.

London Economics. (2017). Analysis of the potential economic impact of GDPR. https://londoneconomics.co.uk/blog/publication/analysis-potential-economic-impact-gdpr-october-2017/. Accessed 26 February 2019.

Martin, N., Bile, T., Nebel, M., Bieker, F., Geminn, C., Hansen, M., Roßnagel A., Schöning C. (forthcoming). Das Sanktionsregime der Datenschutz-Grundverordnung: Auswirkungen auf

Unternehmen und Datenschutzaufsichtsbehörden. Karlsruhe: Forum Privatheit.

Martin, N., & Matt, C. (2018). Unblackboxing the Effects of Privacy Regulation on Startup Innovation, *Proceedings of the 2018 International Conference on Information Systems (ICIS)*, San Francisco, USA.

Matt, C. & Peckelsen, P. (2016). Sweet idleness, but why? How cognitive factors and personality traits affect privacy-protective behavior. *Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS)*, Kauai, HI, USA.

Morlok, T., Matt, C., & Hess, T. (2018). Perspektiven der Privatheitsforschung in den Wirtschaftswissenschaften. In M. Friedewald (Ed.), *Privatheit und selbstbestimmtes Leben in der digitalen Welt, DuD-Fachbeiträge* (pp. 179–220). Wiesbaden: Springer Vieweg.

Myers, M. (2009). *Qualitative research in business & management*. Thousand Oaks: Sage.

OECD. (1997). Regulatory reform and innovation. https://www.oecd.org/sti/inno/2102514.pdf. Accessed 26 February 2019.

Ollinger, M., & Fernandez-Cornejo, J. (1998). Innovation and regulation in the pesticide industry. *Agricultural and Resource Economics Review, 27*(1), 15–27.

Porter, M., & van der Linde. (1995). Toward a new conception of the environment-competitiveness relationship. *The Journal of Economic Perspectives, 9*(4), 97–118.

PWC. (2016). Data breach notification: 10 ways GDPR differs from the US privacy model. https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html. Accessed 26 February 2019.

Ramboll Management. (2005). Economic evaluation of the data protection directive 95/46/EC. http://ec.europa.eu/justice/policies/privacy/docs/studies/economic_evaluation_en.pdf. Accessed 26 February 2019.

Reay, I., Beatty, P., Dick, S., & Miller, J. (2013). Privacy policies and national culture on the internet. *Information Systems Frontiers, 15*(2), 279–292.

Rennings, K., & Rammer, C. (2011). The impact of regulation-driven environmental innovation on innovation success and firm performance. *Industry and Innovation, 18*(03), 255–283.

Schütz, P. (2018). Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich. In A. Roßnagel et al. (Eds.), *Die Zukunft des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung* (pp. 251–268). Wiesbaden: Springer Vieweg.

Stewart, L. A. (2010). The impact of regulation on innovation in the United States: A cross-industry literature review. http://www.itif.org/files/2011-impact-regulation-innovation.pdf?_ga=2.205333144.926975793.1525166652-1519522663.1525166652. Accessed 26 February 2019.

Sun, Y., & Upadhyaya, S. (2015). Secure and privacy preserving data processing support for active authentication. *Information Systems Frontiers, 17*(5), 1007–1015.

Waldman, A. E. (2018). Designing without privacy. *Houston Law Review, 55*(3), 659–672.

Wallace, N. & Castro, D. (2018). The impact of the EU's new data protection regulation on AI. https://www.datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/. Accessed 26 February 2019.

Walz, R., Ragwitz, M., & Schleich, J. (2008). Regulation and innovation: The case of renewable energy technologies. 2008 DIME Conference on Environmental Innovations, Karlsruhe, Germany.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418.

Nicholas Martin is a Senior Researcher at the Fraunhofer Institute for Systems and Innovation Research ISI in Karlsruhe, Germany. He holds a Ph.D. in Political Science from MIT. His research interests include regulation and its impacts on firm behaviour, including innovation, digital business models and data protection.

Christian Matt is an Assistant Professor of Management Information System at the University of Bern, Switzerland. He holds a Ph.D. in Management from LMU Munich, Germany and was a visiting scholar at the National University of Singapore and the Wharton School of the University of Pennsylvania. His current research focuses on corporate digital transformation and digital value creation, data-based services and privacy, as well as on digital customer interfaces and experiences.

Crispin Niebel holds an MSc degree from the University of Kassel and an MA degree from the University of London (SOAS). Currently, he is a PhD degree candidate and part of the *Deutsche Forschungsgemeinschaft* (DFG) Graduate School "Innovative Society today" at the Technical University of Berlin. His research interests include data protection, regulation and innovation.

Knut Blind holds since 2006 the Chair of Innovation Economics at the Technical University of Berlin. Recently, he joined the Fraunhofer Institute for Systems and Innovation ISI as coordinator of the business unit "Innovation and Regulation". Between 2010 and 2019 he was senior researcher at the Fraunhofer Institute of Open Communication System FOKUS. He also held the Endowed Chair of Standardization at the Rotterdam School of Management at the Erasmus University between 2008 and 2016. His research interests include innovation and regulation, including standardization.