Privacy at the intersection of technology, business and regulation

A case study of the GDPR

Gerard Buckley

A thesis presented for the degree of
Doctor of Philosophy

Department of Computer Science
University College London (UCL)

Student declaration

I, Gerard Buckley, confirm that the work presented in my thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Acknowledgements

I'd like to thank my two supervisors, Dr. Ingolf Becker and Dr. Tristan Caulfield. It would not have been possible without them.

As the primary supervisor, Ingolf helped me every step of the way, and he was a pleasure to work with. Tristan offered complementary big-picture support and was a fun mentor.

I'd like to thank Professors David Pym, Madeline Carr, and Shane Johnson for accepting me onto the programme and helping me at various stages of the journey.

I want to thank the course administrator, Fionna Manion, who encouraged me to apply to join the programme when I was hesitant.

I want to thank my cohort, particularly Stefanos Evripidou, Kart Padur, Emmanouil Koulas and Sarah Zheng, for their support.

I want to thank my wife, Sarah and children, Aoife and Ciarán, for putting up with me throughout.

Finally, I'd like to dedicate this thesis to my parents, who always wanted me to be a doctor... of medicine.

Abstract

Technological advances have outpaced privacy safeguards, enabling unprecedented corporate and government surveillance that threatens fundamental human rights. Individuals can counter with privacy-enhancing technologies (PETs) and legal options but face an unequal battle. This thesis investigates the effectiveness of the General Data Protection Regulation (GDPR) in redressing this power imbalance by analyzing its impact on key stakeholders since 2018.

First, it presents new insights into why business embraced the GDPR. While the benefits to consumers (increased rights) and regulators (stronger powers) are well-documented, the upside for business is less understood. Interviews with senior executives reveal that the threat of fines acted as a catalyst for data infrastructure modernization, strengthening the compliance function and yielding multiple direct and indirect benefits.

Second, a consumer survey investigates if those who had worked before, during, and after 2018 in companies that had implemented the GDPR perceived the regulation as beneficial in hindsight. Findings show the regulation sensitized employees to responsible data management within their companies, raising expectations of companies at large. This, in turn, cultivated public support.

Third, the research expands our understanding of how regulators are judged. Surveys and interviews with information security executives, digital rights advocates, and regulators unpack subjective effectiveness assessments. A crucial finding is the weak feedback loop: regulators lack robust accountability mechanisms. The thesis proposes standardized reporting practices and Key Performance Indicators (KPIs) to facilitate benchmarking and improve transparency.

Finally, new ground is broken by imagining the evolution of the GDPR using future-thinking theory. It identifies four lead indicators to monitor and forecast its positioning and relevance in changing environments. Overall, this thesis deepens our understanding of the success of the GDPR model. It sheds light on the factors underpinning its ongoing support by stakeholders and proposes a framework for evaluating future data protection regulator performance.

Impact statement

Privacy is a fundamental human right that is increasingly under threat as technology outpaces existing safeguards. Governments and corporations now possess unprecedented surveillance capabilities, enabling them to monitor the intimate details of our lives, from communications and online activities to travel movements and health data. This accumulated data can be exploited to unduly influence individuals and/or expose them to blackmail or fraud if it is part of a data breach. In theory, privacy laws exist to address this power imbalance.

The General Data Protection Regulation (GDPR) is widely regarded as the world's most important data privacy law and aims to grant individuals control over their personal data. This thesis assesses the GDPR's effectiveness in achieving this goal by analyzing its impacts on key stakeholders in the data economy since it took effect in 2018.

The thesis presents four works, three of which have been published in peer-reviewed international workshops and high-tier academic journals. These works translate empirical analysis into insights on how the GDPR has overcome the usual barbs against bureaucracy, earned recognition as a successful regulatory model that has influenced similar regulations beyond the EU, and become a blueprint for designing future digital regulation within Europe.

First, my research revealed an unexpected benefit: the GDPR provided businesses with a rationale to adopt robust data practices and invest in secure infrastructure, driven by the threat of fines and reputational damage. Regulation put data protection on the Board agenda, empowered the compliance function and engendered positive behavioural change within organizations.

Second, the GDPR sensitized employees to how their employers handled client data more carefully, raising expectations for how other companies should manage their personal data. This fostered support for the regulation among the general public.

Third, my research exposed significant disparities in how regulators implemented the GDPR across the EU, despite it being a supposedly homogeneous regulation. We propose new reporting practices and a set of Key Performance Indicators (KPIs) to facilitate inter-regulator benchmarking and transparency.

Finally, my paper on the future shape of the GDPR identifies lead indicators to monitor and forecast its potential evolution over the next decade. It touches on the status of international data deals, fines, harmonized enforcement, the positive case for regulation, and the need to anticipate that regulation will consistently lag new technologies.

For policymakers and legislators, my research highlights the importance of engaging with business to gain buy-in to a new regulation. For the information security community, the findings demonstrate the value of complementary approaches to preserving privacy beyond privacy-enhancing technology. Ultimately, regulations that reform business practices and rebalance power asymmetries may offer more profound safeguards to society than technically-focused point solutions.

Collectively, this thesis exemplifies how cross-disciplinary work at the intersection of technology, business, and law can generate invaluable insights that enable us to prepare for the future, make better decisions, and develop strategies to mitigate threats to our privacy.

UCL Research Paper Declaration Form

Referencing the doctoral candidate's own published work(s).

For a research manuscript that has already been published:

1. **What is the title of the manuscript?** 'It may be a pain in the backside but...' Insights into the resilience of business after GDPR
2. **Please include a link to or doi for the work:** https://doi.org/10.1145/3584318.3584320
3. **Where was the work published?** NSPW '22: Proceedings of the 2022 New Security Paradigms Workshop
4. **Who published the work?** Association for Computing Machinery (ACM), New York, NY, United States
5. **When was the work published?** June 2022
6. **List the manuscript's authors in the order they appear on the publication:** Gerard Buckley, Tristan Caulfield, Ingolf Becker
7. **Was the work peer reviewed?** Yes
8. **Have you retained the copyright?** Yes
9. **Was an earlier form of the manuscript uploaded to a preprint server (e.g. medRxiv)? If 'Yes', please give a link or doi** Yes: https://arxiv.org/abs/2110.11905

For multi-authored work, please give a statement of contribution covering all authors : The first author conceptualised the study, developed the task, collected and analysed all data, and wrote the manuscript. The senior authors provided guidance during the study design and analysis, provided feedback on earlier manuscript versions and formatted the final version for publication.

In which chapter(s) of your thesis can this material be found? Chapter 4

e-Signatures confirming that the information above is accurate
Candidate: Gerard Buckley
Date: 27 September 2024

Supervisor/Senior Author signature (where appropriate)**:** Ingolf Becker
Date: 3 October 2024

For a research manuscript that has already been published to a pre-print server:

1. **What is the title of the manuscript?** GDPR: Is it worth it? Perceptions of workers who have experienced its implementation
2. **Please include a link to or doi for the work:** https://doi.org/10.48550/arXiv.2405.10225
3. **When was the work posted to the pre-print server?** May 2024b
4. **List the manuscript's authors in the order they appear on the publication:** Gerard Buckley, Tristan Caulfield, Ingolf Becker

For multi-authored work, please give a statement of contribution covering all authors: The first author developed the experiments, collected and analysed the data and wrote the submitted manuscript. The second and third authors provided overall guidance during pilot studies and feedback on earlier manuscript versions. The third author developed the python programs to supplement and extend the in-built analytics on the Qualtrics survey platform.

In which chapter(s) of your thesis can this material be found? Chapter 5

e-Signatures confirming that the information above is accurate (this form should be co-signed by the supervisor/ senior author unless this is not appropriate, e.g. if the paper was a single-author work)**:**

Candidate: Gerard Buckley
Date: 27 April 2024

Supervisor/Senior Author signature (where appropriate)**:** Ingolf Becker
Date: 3 October 2024

For a research manuscript that has already been published:

1. **What is the title of the manuscript?** GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved?
2. **Please include a link to or doi for the work:** https://doi.org/10.1093/cybsec/tyae017
3. **Where was the work published?** Journal of Cybersecurity, Volume 10, Issue 1, 2024
4. **Who published the work?** Oxford Academic
5. **When was the work published?** 10 September 2024a
6. **List the manuscript's authors in the order they appear on the publication:** Gerard Buckley, Tristan Caulfield, Ingolf Becker
7. **Was the work peer reviewed?** Yes
8. **Have you retained the copyright?** Yes
9. **Was an earlier form of the manuscript uploaded to a preprint server (e.g. medRxiv)? If 'Yes', please give a link or doi** No. *I acknowledge permission of the publisher named under 1d to include in this thesis portions of the publication named as included in 1c.*

For multi-authored work, please give a statement of contribution covering all authors: The first author conceptualised the study, developed the task, collected and analysed all data, and wrote the majority of the manuscript. The senior author provided guidance during the study design and analysis, provided feedback on earlier versions of the manuscript and formatted the final version for publication.

In which chapter(s) of your thesis can this material be found? Chapter 6

e-Signatures confirming that the information above is accurate
Candidate: Gerard Buckley
Date: 27 September 2023

Supervisor/Senior Author signature (where appropriate)**:** Ingolf Becker
Date: 3 October 2024

For a research manuscript that has already been published:

1. **What is the title of the manuscript?** How might the GDPR evolve? A question of politics, pace and punishment
2. **Please include a link to or doi for the work:** https://doi.org/10.1016/j.clsr.2024.106033
3. **Where was the work published?** Computer Law & Security Review, Volume 54
4. **Who published the work?** Elsevier
5. **When was the work published?** September 2024c
6. **List the manuscript's authors in the order they appear on the publication:** Gerard Buckley, Tristan Caulfield, Ingolf Becker
7. **Was the work peer reviewed?** Yes
8. **Have you retained the copyright?** Yes
9. **Was an earlier form of the manuscript uploaded to a preprint server (e.g. medRxiv)? If 'Yes', please give a link or doi** Yes: https://papers.ssrn.com/abstract=4830619.

For multi-authored work, please give a statement of contribution covering all authors: The first author conceptualised the study, developed the task, collected and analysed all data, and wrote the majority of the manuscript. The senior author provided guidance during the study design and analysis, provided feedback on earlier versions of the manuscript and formatted the final version for publication.

In which chapter(s) of your thesis can this material be found? Chapter 7

e-Signatures confirming that the information above is accurate
Candidate: Gerard Buckley
Date: 27 September 2024

Supervisor/Senior Author signature (where appropriate)**:** Ingolf Becker
Date: 3 October 2024

Contents

List of Figures

List of Tables

Chapter 1

Introduction

"All human beings have three lives: public, private, and secret."

Gabriel García Márquez: a Life

Technology is outpacing privacy. Governments and corporations now wield unprecedented surveillance capabilities, enabling them to monitor the most intimate aspects of our lives: from our communications, travel movements, online activities, and purchases to even our health conditions. This widespread data collection significantly threatens fundamental rights such as privacy, free speech, security, and equality. The central research question is: *how do we, as a society, take back control of our personal data.* Responses to this challenge within the information security community range from exhorting individuals to adopt privacy-enhancing technologies (PETs) to urging legal action against companies for misusing personal data. This creates a David and Goliath (Schneier, 2015) contest between consumers and corporations. In theory, data protection regulations should offer a solution by rebalancing this power dynamic in favour of individuals via regulatory oversight and intervention. In practice, the picture is less clear-cut. The General Data Protection Regulation (GDPR) is widely regarded as the leader in this field. It has had a major influence on global privacy regulation, and its principles and framework have been copied by countries far beyond European borders. Given the GDPR's centrality to the overarching research question, this thesis aims to assess the effectiveness of the GDPR in protecting individual privacy by analyzing its current and potential impacts on the principal stakeholders in the data economy since it took effect in 2018.

As an engineer and not a lawyer, I initially thought privacy and data protection were synonymous. Not so. For now, let us say that privacy or data privacy is the preferred term in the United States (U.S.). Although not explicitly mentioned in the U.S. Constitution, a penumbral right of privacy has been interpreted as encompassed within the Bill of Rights (Madison, 1792), protecting against unwarranted governmental intrusion into domains such as marriage and contraception. In contrast, Europe enshrines privacy and data protection as distinct yet interrelated rights within the European Union (EU) Treaties and the EU Charter of Fundamental Rights (FRA, 2009). Privacy is regarded as

an integral facet of human dignity, while data protection governs the processing and transfer of individuals' personal data within the EU. Curiously, the term 'privacy' is conspicuously absent from the GDPR text, barring references to another law, the ePrivacy Directive. In this thesis, unless necessary for technical reasons, I use the terms interchangeably, reflecting their conflation in everyday language.

1.1 *"In dreams begin responsibility"*

W.B. Yeats

To paraphrase Yeats's quote, if the dream is to regain privacy, the responsibility to make it happen sits squarely with society, i.e. how do we take back control of our informational privacy at the nexus of fast-moving technology, business interests and data protection regulation? The methodology and methods we use to analyse this central research question depend on the ontological and epistemological perspectives we bring to the study.

Ontology deals with the nature of reality and existence. Here, I veer towards constructivism as it emphasises the role of human interpretation and the social construction of reality. While it may be tempting to adopt a realist worldview and believe a regulation such as the GDPR has an objective reality and allows for empirical investigation, rules do not exist independent of human perception and interpretation and may overlook subjective experiences and cultural variations (Jonker & Pennink, 2010). Constructivism, on the other hand, recognises the role of human interpretation and social construction of reality, promoting a deeper understanding of diverse perspectives but challenging the notion of an objective reality (Jonker & Pennink, 2010). The constructivist view uses qualitative methods. However, I was not averse to taking a mixed or pragmatist approach when some quantitative data was accessible, which enabled me to put my qualitative findings in context.

Epistemology focuses on the nature and scope of knowledge and how it can be obtained. Here, I lean towards interpretivism, acknowledging the subjectivity of knowledge and valuing qualitative research methods. Positivism emphasises empirical evidence and scientific methods, ensuring rigour and generalizability, but it may neglect subjective aspects and complex social dynamics. Interpretivism values subjective experiences and context, facilitating a nuanced understanding, yet findings may be less generalizable and subject to researcher bias (Jonker & Pennink, 2010). This interpretative perspective aligns more with my research goal because I am interested in the perceived effectiveness of the GDPR through the lens of three key stakeholders—business, user, and regulator—and if they believe it has successfully met its objectives.

The ontological and epistemological perspectives shape the research design, methodology, and data collection techniques. Thus, my constructivist and interpretative view suggests methodology choices such as case studies, surveys & grounded research and method tools that include questionnaires, surveys or a mix of both. As I walk through the outline of the thesis, I will highlight and explain the thinking and justification behind the methods chosen.

The background in Chapter 2 sets the scene by summarising the literature on the abstract concept of privacy, the main players in the data economy and the need for protection. It recaps the theory of regulation, the evolution of data

protection regulation in Europe, the GDPR and finally a comparative analysis of the other two significant global data protection regimes in the U.S. and China.

The literature review in Chapter 3 covers the lack of documented benefits from GDPR to business before this research, the scarcity of research into whether employees who had experienced the GDPR implementation think it was worth it or not, an absence of means to assess GDPR regulator performance and a reluctance by commentators to predict the future of the GDPR in five or ten years. These gaps inform the empirical work in this thesis.

In Chapter 4, I explore the impact of the GDPR on business to understand why and how businesses would willingly comply with the rules and not game the system. Before its launch, the literature on the GDPR was full of learned predictions of the benefits and drawbacks of the forthcoming regulation to the world of business and commerce. Post-launch, I found little documentation of concrete benefits to business. This lack of interest in the pain (or gain) of business by the academic community intrigued me. After all, the success of the GDPR relies on business to embrace it. This gap in knowing if and how the GDPR had delivered benefits motivated the first phase of my research, yielding unexpected findings. To realise this exploratory research, my method tool of choice was semi-structured interviews. It has the advantage of uncovering new insights and patterns, a deeper understanding of motivations and behaviours and the flexibility to refine research questions on the fly. It is not without its drawbacks, which I describe in more detail in Section 4.4.4.

Next, in Chapter 5, I focus on the experience of another principal stakeholder: the informed individual. GDPR awareness studies of consumers abound but what I wanted to know was what success means to people in the know, namely individuals who have operationalised it at work whilst simultaneously being beneficiaries of its protections as consumers. Put simply, did they think it was worth it? Surprisingly, audits overlooked this informed community of individuals, possibly because they are not a distinct special interest group, which motivated the second targeted survey-based research. This survey method was chosen because it lends itself to gathering data on attitudes, opinions and demographics on a large sample scale. It allows for better generalizability and lends itself to statistical analysis. As with the interview method, it is not without disadvantages which are described in more detail in Section 5.4.9.

Next, in Chapter 6, I focus on the regulator. Ultimately, a regulation is only as good as how it is executed. And if 'good regulation' is contestable, how does one judge or measure a regulator's performance? Legal literature has avoided setting down precise milestones beyond enumerating lists of desirable qualities. No literature exists on how to benchmark data protection regulators. This motivated the third area of research which involved interviewing hard-to-reach regulators and industry practitioners as well as large-scale surveying of CISOs. The mixed-method approach used here was chosen to capitalise on the strengths of the methods in the two previous studies and mitigate their weaknesses.

Finally, in Chapter 7, having examined the performance of the GDPR to date in the eyes of its principal stakeholders, the next logical question was to explore what was in store for the GDPR in terms of future directions. The literature on the future is wanting. Academic studies oscillate between overly broad and overly narrow analyses. Regulator communications are highly constrained as they refrain from open speculation. Political and campaigner op-eds lack impartiality, and commentary by law firms tends toward soft marketing.

To address how the GDPR might evolve more systematically, I review the main competing data protection regimes to identify the drivers and trends in the regulatory landscape. Combining these generates a series of plausible scenarios that, in turn, inform how the GDPR might have to adapt to handle them. To realise this thought piece without data, I use a PESTLE framework grounded in the background and literature chapters to analyse the political, economic, sociological, technological, environmental and legal factors that may affect the GDPR.

1.2 *"There is no such thing as free regulation."* *John Hutton*

In Chapter 4, I begin by observing that regulation has long suffered an image problem for being dull and unnecessary. And while this can be true, regulation is a vital lever of government policy to deliver better economic, environmental, and societal outcomes. The EU's GDPR is an example of this in the context of data privacy and security. Most attention has concentrated on the benefits of GDPR to the regulator in terms of stronger powers and to the consumer in terms of stronger privacy rights. What we were interested in exploring, however, is whether there are any benefits of GDPR to business and how they might affect the different parts of an organisation. After all, it is business that has to incur the cost to comply with it. Prior to the introduction of GDPR in May 2018, academic literature proposed various potential GDPR benefits to business including better data management and analytics, brand enhancement and access to a level playing field. Since then, however, interest in the business perspective has waned, and it lacks empirical follow-up data. Using semi-structured interviews, I surveyed 14 senior executives responsible for business, finance, marketing, law or IT from 6 small, medium and large companies in the UK and Ireland. To obtain a fuller picture, I deliberately sampled beyond the IT department, which tends to be the typical target of GDPR surveys. I investigate what are the perceived benefits of GDPR to business and where its effects are felt within a business.

We find the threat of large fines has focussed the minds of business and made it more privacy conscious. GDPR has gifted companies a reason to justify investment in modernising their data management processes and security. Companies have cleaner and more up-to-date customer databases. In the absence of GDPR, companies admit they would ask for more information than necessary, use it more frequently, hold it for longer and keep it less securely. It has created new power bases within organisations that act as guardians or champions of privacy. Such in-house regulators will continue to enjoy influence on corporate decision making provided the regulators maintain a steady news flow on enforcement actions against offenders and data breaches. In summary, GDPR may be a headache to business but it has made it more careful with data. Judged by that standard, GDPR has been a successful socio-technical regulation because it has made companies put their house in order to their own benefit and to the benefit of wider society.

1.3 *"Regulations force people to do better"*
Jay Leno

In Chapter 5, I analyse the unique dual perspective of individuals who have had to implement the GDPR in their workplace and who also benefit from it as consumers. Unlike previous perception studies that focused solely on consumers or data professionals, this is the first empirical research into how these informed individuals perceive the cost-benefit of their rights as consumers balanced against the pressures they see it places on their employer to support those rights. With the benefit of hindsight, I ask them if they think it was worth it.

In a multi-stage study, I survey N = 273 & 102 individuals who remained working in the same companies before, during, and after the implementation of GDPR. The literature review has revealed six hypotheses for study:

1. Consumers are aware and knowledgeable about the GDPR.
2. Consumers lack awareness and knowledge about the regulator.
3. Consumers feel their privacy is better since GDPR was introduced.
4. Companies have responded to GDPR and made changes.
5. Employees lack awareness of the GDPR regulator at work.
6. Employees have seen little benefits to their company from GDPR.

The survey finds that participants recognise their rights when prompted but know little about their regulator. They have observed concrete changes to data practices in their workplaces and appreciate the trade-offs. They take comfort that their personal data is handled as carefully as their employers' client data. The very people who comply with and execute the GDPR consider it to be positive for their company, positive for privacy and not a pointless, bureaucratic regulation. This is rare as it contradicts the conventional negative narrative about regulation. Policymakers may wish to build upon this public support while it lasts and consider early feedback from a similar dual professional-consumer group as the GDPR evolves.

1.4 *"Quis custodiet ipsos custodes?"*
Juvenal: Satires

In Chapter 6, I shift the focus away from the target of the GDPR (i.e. business and individuals) to the regulators who oversee and enforce it. The success of any regulation, however good, ultimately depends on how well it is executed. Existing literature fails to answer what good execution means in this context. We research what people think are the objectives of data protection regulators and how they evaluate their effectiveness.

Performance measurement of regulators is challenging due to the indirect nature of their involvement. Their desired outcomes, such as consumer or environmental protection, are not theirs to deliver but are realised by the organisations they oversee. Many external factors can be beyond regulators' control, and outcomes often do not become evident for several years. Assessing the performance of GDPR regulators, where the very concept of privacy is contestable, brings added complexity. Differences in national laws, administrative processes and historical engagement with industry mean DPAs come to GDPR from different starting points. Differences in human and financial resources mean that

DPAs have varying organisational capacities. And differences in political influences mean DPAs' self-confidence and understanding of their role may differ significantly between European countries. All these factors contribute to the noticeably different implementations of the GDPR. Metrics, where available, are often defined differently and make comparative analysis problematic. Such complexity may explain the surprising scarcity of prior research.

We explore novel ways to assess regulator performance more systematically. We surveyed 70 Chief Information Security Officers (CISOs) and conducted 23 structured interviews. The interviewees included informed business executives, lawyers, digital rights activists, and four national regulators. We supplement this with an analysis of diverse enforcement databases. I investigate how the effectiveness of the GDPR regulator is judged and how we could better measure their performance.

Our findings indicate a mismatch between the broad presumed objectives attributed to regulators and the narrow criteria used to judge them in practice. Perception of the regulator's effectiveness is subjective, sanctions-focused and influenced by one's role and responsibilities. Moreover, the independence of regulators, intentionally designed to insulate them from daily politics, raises serious questions of accountability. Lastly, we contribute a series of key performance indicators and make structural suggestions around centralised and standardised reporting of cases to deliver improved learning, legitimacy, transparency and comparability. We believe our findings have important implications for the future development of regulator assessment and accountability in Europe and in the growing number of GDPR-like regimes outside Europe.

1.5 *"Secrets are lies, Privacy is theft"*

Dave Eggers: The Circle

The leadership of the GDPR on global privacy regulation can be seen by how many countries outside of Europe have more or less copied it. The GDPR's pragmatic design, balancing the needs of various EU member states and translated into numerous languages, has fueled its global influence. Given its importance, I decided in Chapter 7 to explore where the GDPR will be positioned vis-à-vis the other major data protection regimes in the next decade and the potential impact it may exert on them. I analyze U.S., Chinese and European approaches (self-regulation, state control, arms-length regulators) through the lens of a political, economic, sociological, technological, environmental and legal (PESTLE) framework. I identify four key drivers shaping the future regulatory landscape: the global battle for influence over cross-border data flow agreements, the "regulation stifles innovation" narrative debate, the challenge of keeping up with fast-moving technology like AI and the struggle of EU national regulators to coordinate and enforce sanctions against well-funded Big Tech. Six potential future scenarios for the GDPR are envisioned, ranging from visions of near-total data sharing to models empowering individuals. While a minor update to the status quo version is most likely, I argue a stronger application is needed, requiring stricter penalties for non-compliance, public censure, defence of cross-border data rights, and proactive guidelines for emerging technologies. Strengthening the GDPR's effectiveness is crucial to ensure the digital age empowers individuals, not just information technology corporations and governments.

1.6 *"The pen is mightier than the sword"*

Edward Bulwer-Lytton: Cardinal Richlieu

In Chapter 8, I reflect that when I began my Masters in Information Security at UCL I was convinced the answer to problems caused by technology was better technology. In particular, I believed the solution to over-intrusive Big Tech was privacy-enhancing technology (PET) partly because I was conscious that technological innovation was outpacing the ability of law to keep up. I soon discovered that even the ICO did not regard PET as a silver bullet (ICO, 2018a). For my MSc dissertation, I studied data trusts, quasi-PET and legal structures that attempted to take back control. I discovered they had potential but their long-term effectiveness remained unproven. As I progressed in my PhD studies of the central research question, I came to a different conclusion. PET will be part of the solution, but regulations will have a more powerful, longer-lasting impact on technological abuse by Big Tech than PET, just as anti-trust laws affected Big Oil and Big Railroads. I have demonstrated that a data protection regulation like the GDPR, however imperfect, has encouraged mainstream companies to become more privacy-conscious and, belatedly, Big Tech. It has made the general public more aware of their rights and given regulators more confidence to resist corporate lobbying pressure. Overall, this thesis deepens our understanding of the GDPR model's success. It sheds light on the factors behind its ongoing support by stakeholders and proposes a framework for evaluating future data protection regulator performance. These studies give the information security community a more rounded understanding of the path to protect privacy at the intersection of technology, business and regulation.

Chapter 2

Background

In this chapter, I introduce the concepts of privacy and regulation and how they combine to create data protection regulation. There are four sections. First, I provide a concise overview of the literature on the difficult-to-define idea of privacy and its historical transformations. Second, I review the data economy, the roles of various stakeholders in the data economy and the extent to which individuals have privacy today. Third, I summarise briefly the fundamental theory of regulation, the principles of good regulation, and different regulatory approaches. Lastly, I analyze the evolution of data protection regulation, particularly the General Data Protection Regulation (GDPR), and its position relative to the U.S. and Chinese regulatory frameworks. This legal overview is intended to provide a contextual backdrop for the research questions rather than a comprehensive summary.

2.1 Privacy is a contested concept

While the general public uses the terms interchangeably, privacy and data protection are technically different concepts. The word 'privacy' does not appear anywhere in the GDPR (apart from a reference to the ePrivacy Directive). Data protection is a relatively modern term we will define more precisely in Section 2.4.3. Semantics aside, the overlap in common understanding highlights the complex interplay between privacy and technology.

Defining privacy has challenged scholars since time immemorial. It has moved from the hands of philosophers to lawyers and social scientists. Early reflections on privacy hark back to Athens and the philosophers' distinction between the public sphere of political activity and the private sphere of domestic life. It was not until the emergence of classical liberalism in the seventeenth century that the right to privacy was raised by the English philosopher John Locke in his Two Treatises of Government, where he argued that the right to privacy is a natural right that is necessary for the preservation of liberty (Cloud, 2018; Locke, 1689). By the eighteenth century, English common law defined the right to privacy in the form of the inviolability of one's property "for a man's house is his castle, for safety and repose to himself and his family" (Vickery, 2008). As technology advanced, privacy and the way it could be violated changed. In 1891, the American lawyers Samuel Warren and Louis Brandeis (Warren & Brandeis,

1890) described the right to privacy in a famous article: The right to be let alone.

In 1948, the right to privacy was established by the United Nations (United Nations, 1948). Article 12 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Coincidentally, George Orwell's novel 1984 was published in the same year.

In 1960, William L. Prosser (1960) published a landmark article on tort law that outlined four privacy harms: intrusion upon seclusion or solitude, or into private affairs; public disclosure of embarrassing private facts; publicity which places a person in a false light in the public eye; and appropriation of one's name or likeness. Westin reinterpreted it at the onset of the computer age as "the claim of individuals ... to determine for themselves when, how and to what extent information about them is communicated to others" (T. Davies, 1999; Kumaraguru & Cranor, 2005). Ferdinand Schoeman (1992) expanded it to mean a system of norms that protect social freedoms and self-expression. Solove (2008) believed that "Privacy is the relief from a range of kinds of friction". He created a six-dimensional model to describe privacy and developed a legalistic taxonomy of consequential harms caused by privacy violation. Conversely, Ken Gormley (1992) argued it was a misguided quest to seek one-size-fits-all definition of privacy because privacy is sensitive to "historic jolts or catalysts that produce new brands of privacy each time the law is faced with unexpected social or technological change".

Westin (Kumaraguru & Cranor, 2005) created a Privacy Segmentation Index to measure people's attitudes to privacy. It is still a popular model today, although its relevance to the digital world has been questioned since it predated the existence of social media and mobile phones. The gap between people's words and actions in the context of active privacy protection (aka the privacy paradox) is a well-known phenomenon (Ackerman et al., 1999). Multiple surveys by the Pew Research Centre (Auxier et al., 2019; Madden & Rainie, 2015) show that a majority of Americans think their personal data is less secure now and have little faith that social media executives will protect user privacy. An international survey of 20 countries showed users trust in the internet had dropped significantly since 2019 (IPSOS, 2022).

In 2004, Nissenbaum (2004, 2011) introduced "the framework of contextual integrity" that saw privacy as "neither a right to secrecy nor a right to control but a right to appropriate flow of personal information". Appropriateness depends on the situation. Doctors can ask you for personal medical information but not your salary details. Bankers can ask you for sensitive financial information but not enquire about your bowel movements. Nissenbaum went further. Privacy is just not about the home. People should have some privacy in public and not be subject to intrusive Big Brother surveillance.

Koops et al. built on this and developed "A taxonomy of Privacy" (2016). They envisaged four zones: a personal solitude zone, an intimacy zone, a semi-private zone and a public zone. They then imagined two horizontal freedom strands where the emphasis was "being let alone" or freedom to "self-development". The former includes bodily, spatial, communicational and proprietary privacy. The latter includes intellectual, decisional, associational and behavioural privacy.

In recent years, the rise of social media, location tracking, cookies, recommender systems etc, has renewed focus on Westin's concept of informational self-determination. Since its original articulation, the biggest change has been the sheer volume of intimate personal data we surrender and allow to be collected by new smart products and services. While the idea of 'state surveillance' and the 'sentinel state' (Pei, 2024) has been known to information security professionals for some time, Shoshana Zuboff (2019b) is widely credited for introducing the term 'surveillance capitalism' into mainstream discourse to describe this loss of control. In response, scholars like Brunton & Nissenbaum (2015) propose obfuscation techniques to counter digital surveillance. Véliz (2021) advances practical measures for reasserting data control, including using privacy-focused search engines, covering webcams, employing VPNs, and choosing non-networked devices. Wachter et al. (2020) and Pasquale (2015) tackle algorithm opacity, while Gasser (2016) and Hartzog (2018) look at recoding privacy law with privacy-enhancing technology and embedding privacy by design in new products. This scholarship contributes to a growing body of research that challenges the privacy-invasive default of our contemporary data-centric technological infrastructure.

To sum up, privacy will continue to be contested because it is open to reinterpretation according to changing technological and societal norms.

2.2 The Data Economy

In this section, I review the literature on who I believe are the three main actors in the data economy: the consumer, Big Tech and the state. In the interests of space and time, I omit less significant stakeholders that have responsibilities under data protection law from the scope, such as charities, local authorities, and community groups. I show that consumers can be their own worst enemy in terms of protecting their data privacy, that the government may not be as trustworthy as assumed, and that Big Tech will continue to collect more and more personal data unless society puts limits on it.

2.2.1 The Consumer

Surveys (Auxier et al., 2019; Faverio, 2023; McClain et al., 2023) consistently show that privacy is a primary concern for citizens in the digital age. Notwithstanding this, individuals reveal personal information for relatively small rewards, often just to draw the attention of peers in an online social network. This inconsistency of privacy attitudes and privacy behaviour is often referred to as the 'privacy paradox'.

The privacy paradox has significant implications for e-commerce, online social networking, and government privacy regulation. The digital economy relies on collecting vast amounts of personal information. If people aren't bothered about privacy, in reality, this plays perfectly to Big Tech's business model. If, on the other hand, people are genuinely concerned, this supports the argument for increased privacy regulation by the government.

While some scholars (Draper, 2017) may take issue with the term paradox, it is incontrovertible that individuals exhibit privacy-sabotaging behaviour daily. Explanations of the privacy paradox are derived from four research areas:

(a) privacy calculus theory, (b) social theory, (c) cognitive biases and heuristics in decision-making, (d) decision-making under bounded rationality and information asymmetry conditions.

Privacy calculus theory postulates that individuals perform a calculus between the expected loss of privacy and the potential gain of disclosure. Their final behaviour is determined by the outcome of the privacy trade-off (Dinev & Hart, 2006; Xu et al., 2011). Despite intangible rewards and quantification challenges, studies show that users of Social Media Sites (SMS) disclose personal information when perceived benefits outweigh observed risks (Debatin et al., 2009; Lee et al., 2013).

Social theory posits that active participation in online social networks, involving self-disclosure, aligns with three fundamental needs: diversion, social relationships, and identity construction (Debatin et al., 2009). The benefits of information sharing that users value the most include self-clarification, social validation, relationship development, social control, and self-representation (Lee et al., 2013). These encompass understanding oneself, affirmation of one's views, deepening relationships, influencing others attitudes or behaviour, and constructing a personal image of oneself.

Social networking is a way of gaining social capital. It refers to the internal social and cultural coherence of society. As such, social capital has been described as a glue. For individuals, social capital is a source of power and influence that helps people to 'get by' and 'get ahead'. Individuals disclose personal information in order to earn social capital. For example, an individual who discloses a medical condition will be more likely to receive more support and sympathy from network members (Stutzman et al., 2012).

Research in behavioural economics has shown that human decision-making is affected by cognitive biases and heuristics (Acquisti & Grossklags, 2005). It is unlikely that privacy decisions are not affected by the same biases and heuristics. The latter include optimism bias, overconfidence, affect bias, fuzzy-boundary and benefit heuristics, and hyperbolic discounting.

Optimism bias refers to individuals consistently believing they are less at risk of negative events than others. Unfortunately, this bias hinders people from protecting themselves from a privacy breach (Baek et al., 2014). The affect heuristic, a mental shortcut, leads individuals to underestimate risks related to things they like and overestimate risks associated with dislikes (Slovic et al., 2007). It influences the assessment of risk and perceived benefits of self-disclosure (Kehr et al., 2013, 2014). When primed with the fuzzy boundary heuristic (Sundar et al., 2013), individuals disclose less personal information, while those primed with the benefit heuristic tend to share more. Additionally, hyperbolic discounting theory suggests that humans inconsistently value the future, often prioritizing immediate gains over long-term protection (Acquisti & Grossklags, 2003). Thus, individuals may express a preference for privacy but prioritize present benefits.

Bounded rationality refers to the cognitive limitations facing a human decision maker: limitations of both knowledge and computational capacity. Thus, their privacy decisions are constrained by incomplete information and bounded rationality (Acquisti & Grossklags, 2005), two conditions that affect decision-making in several contexts (e.g. market trading, business management, etc.).

Information asymmetries prevail in the relationship between consumers and providers in the data economy. For example, mobile phone consumers have

very little knowledge of their apps and how their personal data are used. They consider information from their social group and the app store more important and trustworthy (Buck et al., 2014).

Sharing personal data to access a free service is a form of trade. Acquisti et al. argued that "Privacy is, after all, a process of negotiation between the public and private, a modulation of what a person wants to protect and what she wants to share at any given moment and in any given context" (2016). However, the problem is that many consumers don't realize it's a trade, and even if they did, they don't know the value of their data, so they can't assess if it's a fair exchange. If they refuse to share their data, they'll be denied access to the service, illustrating the power and information asymmetry between the two parties.

There are upsides to sharing personal information. It makes online shopping easier, more convenient, and personalized. Volunteering information can help sellers offer the appropriate product, reducing the buyer's search costs. There are social benefits to being part of an online community. It enables crowding sourcing apps like Waze, where drivers share road traffic updates for everyone's benefit. In fact, it could be argued that not sharing is selfish and a cost to society. According to Posner "protection of privacy can create inefficiencies in the marketplace" (1978, 1981). How could we ever benchmark anything if nobody shared information? Over-protection can impede social progress and the exchange and cross-fertilisation of new ideas.

There are downsides to sharing personal information. It can lead to price discrimination or algo-racism without the individual's knowledge. Over-sharing may also cause unintended harms like reputational damage, embarrassment, social abuse, mental health issues, vulnerability to blackmail and fraud, and economic loss. Once a consumer's data is out there, it is quickly captured and resold by data brokers to various organizations, often for advertising purposes. The consumer has no idea where it ends up.

The privacy paradox explanation is not without critics. In "From Privacy Pragmatist to Privacy Resigned," Draper (2017) challenges the prevailing narrative that there is a paradox or contradiction. She proposed a phenomenon called digital resignation to explain the rational, emotional response when confronted with an undesirable situation that individuals believe they cannot combat. This perspective has similarities to the psychological theory of learned helplessness. People feel resistance is futile, given the pervasiveness of data collection and surveillance and their lack of control over their digital footprints.

In summary, individuals can be their own worst enemies when it comes to protecting their personal privacy despite protests to the contrary. Proposals to limit the harm individuals might cause to themselves generate considerable debate. Some argue that moral and economic imperatives require state intervention while others claim individuals' choices should not be constrained and regularly describe government intervention as 'nanny state'. Opponents of regulation accuse the government of trying to assume a decision-making role they argue belongs to individuals. This assumes a rational choice framework. However, human behaviour research shows that individuals regularly make perverse self-harming choices based on a variety of factors open to manipulation. Commentators, such as Draper (2017), would challenge the choice narrative and characterise the shift in behaviour as a rational response to the data economy. Labelling privacy regulation as 'nanny statist' may posit a false dichotomy be-

tween laissez-faire and intervention, failing to recognize intervention as a means of achieving individual freedom of choice. The GDPR is an example of a regulation whose stated aim is to empower consumers.

2.2.2 Government

Governments, perceived as neutral players in the data economy, are entrusted with designing the 'rules of the game' and regulations. However, history shows that governments and rulers have long been keen collectors of personal data. For instance, after the Norman conquest of England in 1066, William, Duke of Normandy, created the Doomsday Book—a property and population database—for taxation purposes. Today, governments utilize personal data extensively for national identification, e-voting, and public services. While they claim to represent the interests of the people, governments are no longer sole regulators; they also act as data vendors and wield extraordinary surveillance powers in the name of national security. This section explores if our trust is misplaced.

In The Future of Citizen Data Citizens (Government Office for Science, 2020), the UK employs the term 'citizen data' to distinguish it from specific legal definitions of 'personal data'. This distinction is crucial because the concept of personal data evolves over time and varies across jurisdictions, often implying specific rights like ownership. Citizen data encompasses four expanding layers: (i) Citizen Individual Identity Data: This layer includes essential information such as date of birth, address, ID documents, biometric data, medical records, and educational records; (ii) Citizen Generated Data: Here, we find financial data, phone records, and social media activity: (iii) Citizen Observed Data: Tracking cookies, IoT (Internet of Things) data, utility usage records, and CCTV footage fall into this category: (iv) Citizen Aggregated Data & Inferential Data: This layer involves census data, metadata, de-identified records, and advertising profiles.

The volume and variety of citizen data are rapidly increasing. The UK (Government Office for Science, 2020) believes that effectively utilizing and sharing this data can yield substantial benefits for the economy and society, often extending beyond the original data collection purpose. It serves as a fundamental input for economic growth, job support, and productivity. Additionally, citizen data fuels innovation across various sectors and contributes to research for the public good (as exemplified by the UK Statistics Authority). Even data generated and held by private entities can have value beyond its initial purpose. Wider use and sharing of citizen data directly benefit public service users and providers. In healthcare, sophisticated linking and analysis of citizen data can enhance provision and research. Furthermore, broader linkage and re-use of this data play a crucial role in monitoring and evaluating development initiatives

While the widespread adoption of digital identity (eID) systems by governments offers advantages, they also raise critical issues related to power relations between the state and individuals (e.g. the rise of the surveillance state, data justice, and the protection of vulnerable individuals and communities) (Anand & Brass, 2021). Generic risks include segregation, stigmatization, lack of transparency, and inadequate data protection. These concerns are particularly pronounced in countries without robust data protection laws. As eID systems collect more personal data, citizens face a loss of privacy and agency, as these systems become linked to services and analytics platforms that track, exclude or

penalize non-compliant behaviour such as using welfare money to purchase alcohol or gambling products (Arora, 2016). Thus, individuals are vulnerable not only to criminal hackers but also to governments cross-referencing their personal data for social engineering purposes.

State surveillance is as old as civilisation itself. Historically, it involved a spy or a group of spies monitoring the actions of other people (usually enemies). As technology advanced, surveillance practices moved to telescopes, radio and phone tapping, but it still involved a one-to-one relationship between the eavesdropper and the eavesdropped. With the advent of the internet and other advanced information and communications technology (ICT), surveillance changed from targeted data collection to bulk data collection. ICT massively increases the power, reach, and capacity of governments to monitor their populations (Lyon, 2007; Marx, 2015). In political science, research increasingly examines how authoritarian regimes employ surveillance as a tool to counter domestic political threats (Kuran, 1997). Surveillance allows for the detection of dissent and the extraction of intelligence, enabling the targeted repression (Anita R. Gohdes, 2020).

State surveillance is not the sole preserve of authoritarian regimes. In the U.S., privacy is safeguarded by the Fourth Amendment, which protects "papers and effects" within the home but not in "plain view". The National Security Agency (NSA) is tasked, inter alia, with the protection of U.S. communications networks and information systems. By executive order, it is prohibited from "acquiring information concerning the domestic activities of U.S. persons". In 2010, Casper Bowden (2014), former chief privacy advisor at Microsoft, revealed that Section 702 of the U.S. Foreign Intelligence Surveillance Act (FISA) empowered U.S. intelligence to surveil non-US individuals through electronic communications service providers. This surveillance wasn't limited to crime or terrorism; it allowed purely political activities. Bowden's warning about cloud computing and privacy preceded the Snowden leaks, emphasizing the U.S.'s use of European reliance on such services for monitoring non-US citizens (2012). His work shed light on the impact of U.S. surveillance programs on EU citizens' fundamental rights.

In 2013, documents (ACLU, 2013; MacAskill et al., 2013) leaked by Edward Snowden had a transformative effect on law, business practices, and the general public's perception of surveillance. It revealed the power of the NSA's UPSTREAM programme that siphons data flows as they pass through cables and infrastructures, and PRISM collects data directly from the servers of U.S. service providers such as Microsoft, Google, Facebook, Paypal and Apple. In just a short time, between January 2012 and the summer of 2013, the behaviour of the European Parliament (EP) changed. Despite heavy lobbying, the GDPR passed in its first reading, reflecting the preferences of a coalition of privacy advocates.

These surveillance revelations fundamentally changed the substance of the GDPR debate. If before the revelations, the GDPR debate was solely about Internet privacy, now it had become about the protection of Europeans' Internet privacy from unwanted and abusive American surveillance. Attention focused on international data transfers, data protection, and the location of cloud services. Safe Harbour was declared invalid in the first Schrems judgement on 6 October 2015 (CJEU, 2015). Privacy Shield, the successor to Safe Harbor, was ruled invalid in the Schrems II case by the ECJ on 16 July 2020 (CJEU, 2020). This

stand-off has spurred U.S. cloud providers to establish EU-based operations to service European clients in a GDPR-compliant manner (ITIF, 2021). In July 2023, the EU and the U.S. finalised a Data Privacy Framework, which Max Schrems has challenged on similar grounds as in the past (noyb, 2023c).

In summary, people look to the government to protect them from predatory data practices by Big Tech. Simultaneously, governments are increasingly active data players as they digitize service access. Furthermore, some governments purchase supplemental citizen data from private-sector data brokers and even share public data with private entities. The same governments also wield extraordinary surveillance rights, as revealed by the Snowden affair. While surveys show that citizens desire more government intervention to safeguard their data, surveys also reveal a growing trust deficit in Western democracies.

2.2.3 Big Tech

Multiple motivations exist for regulatory intervention. Market failure is the classic justification, and it comes in many guises. I summarise why Big Tech has attracted attention on multiple fronts, including competition and privacy.

At the Hackers Conference in Marin County, California, in 1984, Stewart Brand famously declared, "Information wants to be free" (Levy, 2014). Less well-known, he elaborated: "On the one hand, information wants to be expensive because it's so valuable. The right information in the right place can change your life. On the other hand, information wants to be free because the cost of disseminating it keeps decreasing over time." Steve Jobs advocated using technology to change the world (Isaacson, 2012). Google's original motto was 'Don't be evil,' later revised to 'Do the right thing' (Prager, 2018). Mark Zuckerberg's mission for Facebook is 'Connecting the World' (Muir, 2017). However, such lofty rhetoric rarely acknowledges the source of the tech titans' profits.

In the U.S., 85% of the stock market valuation is concentrated in companies classified as mega-cap or large caps, and most of these companies are intellectual property or IP-rich (CRSP, 2024). Over time, there has been a shift from tangible to intangible wealth, and post the 2008 credit crisis, wealth has moved from financial services to Big Tech. The term 'Big Tech' (Wikipedia, 2024b) first appeared in the media around 2013, and is a loose collective term for high valuation, high market share, or high growth technology companies. In recent years, the dominance of Big Tech has been a growing area of concern for policymakers and the public. For example, Apple, Amazon, Alphabet, Meta, Microsoft, Nvidia, and Tesla account for almost 30% of the market capitalization of the S&P 500 (Fool, 2024).

Big Tech is not a homogenous group, but a number of them, particularly Alphabet and Meta, grew wealthy on the back of an audacious appropriation of users' behavioural data as a free resource, what Shoshana Zuboff calls "Surveillance Capitalism" (2015, 2019a). Sarah Myers West prefers the term 'data capitalism' (2019) to describe the turn from an e-commerce model premised on the sale of goods online to an advertising model premised on the sale of audiences. Personal data is the new oil, and it is virtually cost-free to drill. Imagine how profitable General Motors would be if steel were free. This partly explains why Big Tech has accumulated such vast wealth so fast.

Big Tech's modus operandi involves providing free services to billions of grateful users, surreptitiously recording and analyzing behaviour, often with-

out explicit consent. This trove of data feeds into AI algorithms, generating prediction products that anticipate our actions, from immediate decisions to future milestones like birthdays or policy renewals. Consumer companies willingly pay substantial sums to access these data products, fueling Big Tech's immense wealth. Eric Schmidt, Google's former CEO, once declared a privacy policy "to get right up to the creepy line and not cross it" (Sterling, 2010). However, this boundary has blurred, resulting in a disconcerting reality: Once, we searched Google, but now, Google searches us. Once, we thought of digital services as free, but now digital capitalists think of us as free.

Another element underlying the Big Tech business model is platform capitalism. Platform providers position themselves as intermediaries that bring together different users: customers, advertisers, service providers, producers and suppliers. Central to all of it is data. The fear is that platform providers already enjoy a sustained competitive advantage that will enable these firms to maintain their lock on the market for the near future. Exclusive access to data, exploitative access to information by demanding a quid pro quo from customers, economies of scale and scope, as they move into adjacent markets, network effects, and data-induced switching costs, are all facilitating factors. The fear is that this lock will harm competition and innovation.

To address these fears across Europe, the EU recently introduced the Digital Markets Act (DMA) (2022). It aims to promote fair competition and limit the market power of the largest tech companies ('gatekeepers'). The act imposes serious obligations: companies will have to allow third-party apps and app stores on their platforms; provide transparent advertising data; allow users to uninstall pre-installed software or apps easily; enable interoperability between different messaging services, social networks, and other services, allowing users to communicate seamlessly across platforms; and be more transparent about how their algorithms rank and recommend content, products and services. It also prohibits certain practices by gatekeepers: favouring their own services over third-party ones, for example, engaging in self-preferential activities and using private data from business users to compete against them. In other words, it seeks to put an end to business as usual.

To sum up, the challenge for societies today is not whether they are capable of reining in the immense power of Big Tech. We know this can be done because the Chinese Communist Party has done it. The question is whether liberal democracies are up to the job. The significance of the GDPR and now the DMA is that it's the first time regulators have modernised in combination consumer data protection and competition regulation to tackle the exploitation of data and dataflows: the very foundation of the new data economy's business model.

2.3 Regulation Theory

Regulation theory is a vast field of study. We limit ourselves to a high-level understanding of the motivation behind regulation, what constitutes good regulation and differing regulatory approaches.

2.3.1 The form and function of regulation

According to the OECD, regulation is indispensable to the proper functioning of economies and societies (OECD, 2019) and is a key tool for governments to achieve policy objectives. It refers to the mechanisms by which governments set requirements on businesses, and the term 'regulator' refers to a person or authority who develops or administers regulation.

Governments regulate for many reasons. The technical justification for regulation is that it addresses market failures that are not in the public interest (Breyer, 1982; Mitnick, 1980; A. I. Ogus, 2004) (e.g. monopolies and natural monopolies, externalities, information inadequacies, anti-competitive behaviour and predatory pricing, unequal bargaining power). They are not mutually exclusive, and the case for regulating will often be based on a combination of rationales. Regulation bridges the gap between an operator's profit-orientated self-interest and the interests of society (Williamson et al., 2006).

A classic definition of regulation (Black, 2005) is the "sustained and focused attempt to alter the behaviour of others according to standards or goals with the intention of producing a broadly identified outcome or outcomes", which may involve "mechanisms of standard-setting, information-gathering and behaviour modification".

There are different "types" of regulatory interventions. A simplified taxonomy by Pelkman and Renda (Pelkmans & Renda, 2014) includes regulation through information (e.g. improved transparency), self-regulation (e.g. voluntarily establishing common rules and codes of practice), co-regulation (e.g. a mix of legislation and self-regulation), standardisation (e.g. delegating the detail to standards organisations), market-based instruments (e.g. taxes, charges, licenses, quotas) and prescriptive actions (e.g. traditional 'Command and Control (C&C)' policies and performance-orientated requirements). C&C policies dictate the use of certain practices, technologies, or designs. The advantage is relative ease of monitoring and enforcement. The disadvantages are that they will likely be less cost-effective, discourage technological innovation, or go beyond standards. Performance policies specify the required target performance without detailing the exact mechanisms by which compliance is obtained. Both prescriptive actions rely on hard metrics that can be assessed externally against regulatory targets.

2.3.2 Principles of good regulations

What constitutes 'good regulation' is difficult to establish and is subject to contention by legal scholars. Commentators and governments alike have tended to avoid precise definitions and have preferred instead to enumerate desirable qualities or criteria in a good regulatory regime. What is not vague, however, is that once a new regulation comes into effect, it can have a massive impact on a market.

For this reason, most developed economies have policies, procedures and institutions to govern how regulations are developed, administered and reviewed. While approaches vary, such policies typically affirm the importance of openness, proportionality and fairness (World Economic Forum, 2020).

Openness demands transparency and participation in the policy design to ensure regulation serves the public interest and engages all the stakeholders that

it affects or who hold an interest in it. Proportionality demands that the costs of compliance are commensurate with the benefits the regulation is intended to deliver. Fairness demands that regulatory decisions should be made on an objective, impartial and consistent basis, without conflict of interest, bias or improper influence. The theory is that this enables businesses to compete on a level playing field (LPF), and helps ensure that the best ideas, products and business models are those that succeed (Salter, 2020).

2.3.3 Regulatory approaches

A significant distinction in regulatory approaches lies between principles-based regulations and rules-based regulations (Black, 2007). The former relies on overarching, broad principles often articulated with qualitative terms such as 'fair' or 'reasonable,' alongside explanations of the underlying intent. These principles are crafted to apply across diverse circumstances, prioritizing outcomes over specific inputs. In contrast, rules-based regulation entails precise statements delineating the requirements firms must adhere to, typically employing quantitative terms. In recent years, there has been a notable shift towards principles-based regulation, driven by the belief that it encourages firms to consider the practical implementation of regulations within their operations, rather than merely adopting a superficial compliance mindset. Additionally, principles-based regulation offers the advantage of reduced frequency in updates to respond to evolving circumstances. However, it is not without drawbacks, notably the lack of precise standards for customers or consumers to reference.

Both rules and principles can vary across regulatory regimes. One principle particularly relevant to the subsequent discussion, contrasting three privacy regimes, is the precautionary principle (EUR-Lex, 2002). This principle serves as a risk management approach, stipulating that if a policy or action might potentially cause harm to the public or environment, and scientific consensus is lacking, the activity should not proceed (Thierer, 2014). Notably, it reverses the burden of proof: the agent proposing the activity must prove the activity is not harmful.

In the US, Solove (2020) classifies three dominant approaches shaping privacy:

Self-Management Empowering individuals with control through rights like access, correction, deletion, data portability, opt-in and opt-out. However, public awareness limitations and the impracticality of overseeing diverse platforms hinder its effectiveness.

Governance & Documentation Organizations take responsibility by appointing chief privacy officers, audits, and policies. While essential for compliance, concerns exist about documentation overshadowing substantive protection.

Use Regulation Specific restrictions are placed on data usage for sensitive datasets. Examples include the Fair Credit Reporting Act (FCRA) and the Health Insurance Portability and Accountability Act (HIPAA). While less common, it offers targeted protection.

Although the EU, US and China have different privacy regulatory regimes, all three approach the issue from a consumer protection and market competition perspective while reserving special rights for the state. Policymakers often treat

the two areas separately because market competition/antitrust tends to focus on firm-to-firm interactions, while consumer protection deals with firm-to-consumer interfaces (Jin & Wagman, 2019). The two areas are subject to different laws, and crossovers between the two have tended to be small. However, big data and online platforms blur the distinction between the two and can cause overlap or conflict.

2.4 Data Protection Regulation

In this section, I review the global regulatory landscape in four parts. First, I trace the historical evolution of privacy and data protection in Europe and how the current regulation tries to balance conflicting interests. Second, I summarise the GDPR and highlight its main principles and rights. Third, I look at data protection in the US and China as they vie with Europe to establish the dominant model for regulating technology in the digital economy. Lastly, I focus on the new EU Artificial Act and how it may interact with the GDPR.

2.4.1 The evolution of European privacy and data protection law

The roots of the GDPR can be traced back to two concepts: privacy and data protection. What follows is a short history of the law and the main milestones.

Privacy is covered by Article 8 of the European Court of Human Rights (ECHR) (Hirvelä & Heikkilä, 2022), the Right to respect for private and family life. It says:

> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."*

The ECHR was opened for signature in Rome on 4 November 1950 and came into force on 3 September 1953. It was the first instrument to give effect to and make binding certain of the rights stated in the Universal Declaration of Human Rights (Nations, n.d.). Article 8 sought to protect individuals against undue interference by the state in a person's private life, such as interception of communications or the criminalisation of private sexual acts. However, by the end of the 1970s and early 1980s, the lack of clarity as to the ECHR's horizontal effect meant that individuals were not adequately protected against the abusive collection and use of their data. The threat from computers sparked widespread debate in Germany, Norway, Sweden, France and the UK. The public became sensitised to the potential for privacy infringement enabled by new technology, the repercussions from data mistakes, and authoritarian power risk.

Data protection is covered by Article 8 of the Charter of Fundamental Rights of the European Union (CFR): Protection of personal data (for Fundamental Rights, 2015). It says:

> *"1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."*

In Germany, personal data protection was linked to more expansive, more fundamental societal values. The term informational self-determination became key to understanding the German view of privacy after a constitutional case in 1983 ruled that *"the authority of the individual to decide himself, on the basis of the idea of self-determination, when and within what limits information about his private life should be communicated to others."* Norway, Sweden, France and the UK enshrined the right to data protection as a 'sui generis' (in a class by itself) right, but they did not adopt the German concept of self-determination. They saw data as a valuable resource and subject to competing interests. For them, data protection aims to safeguard a just and reasonable equilibrium between the interests of the individuals and those of the community concerning the processing of personal data as enshrined in the 1980 OECD Privacy Guidelines, 1981 Convention 108 and 1995 Directive 95/46/EC.

The GDPR (EU 2016/679) (EU, 2018h) is a European Union Regulation that replaced and repealed the EU's 1995 Data Protection Directive (DPD, also known as Directive 95/46/EC) (EC, 1995). It talks to *"the protection of individuals with regard to the processing of personal data and on the free movement of such data"* (EU, 2018). This dual mandate explains the mix of prohibition and permission contained in the GDPR. It is prohibitive because it says that personal data cannot be processed unless certain conditions are satisfied, which has echoes of informational self-determination and individual control. At the same time, it is permissive in that it says personal data can be processed provided certain conditions are satisfied. This dual mandate provides a balancing of interests, but it also underlies many of the critiques of the day to day operation of the GDPR, as we will see later.

2.4.2 Privacy v Data Protection

In many contemporary debates on surveillance, information monopolies and the data economy, the terms "privacy" and "data protection" are used interchangeably. While there are overlaps, there are also differences between the scope of both rights rights and limitations (Kokott & Sobotta, 2013).

If privacy and data protection were represented by a Venn diagram, one would observe significant intersection. Both are recognized as fundamental rights in the EU, with overlapping objectives of protecting individuals' personal information and autonomy. Both ECHR and the ECJ play roles in interpreting and enforcing these rights, often treating data protection as an expression of the right to privacy. Both rights aim to safeguard individuals from misuse of their personal information, whether by the state or private entities. Both share common principles such as consent, transparency, and accountability.

Where the Venn diagram does not fully overlap relates to the scope of rights, legal framework and application. Privacy encompasses a range of protections,

including personal autonomy, physical spaces, and personal choices. It is a fundamental right with a long history, primarily aimed at protecting individuals from state interference. Data protection focuses on the control and processing of personal data. It has evolved from international principles and secondary legislation to a fundamental right in the EU, binding both public and private entities. Privacy is rooted in Article 8 of the ECHR, which protects the right to respect for private and family life. Data protection is governed by the GDPR and Article 8 of the EU CFR, which provides a specific and reinforced system of protection for personal data. Privacy can apply to various contexts beyond data, such as physical intrusions or surveillance. Data protection applies specifically to the processing of personal data, regardless of whether there is an interference with the personal sphere.

In EU law, data protection has a precise meaning. It controls the use of personal data, which is any information relating to an identified or identifiable natural (living) person, including names, dates of birth, photographs, video footage, email addresses, and telephone numbers. Other information, such as IP addresses, is also considered personal data.

In summary, privacy is generally regarded as broader, encompassing various aspects of personal autonomy, whereas data protection specifically addresses the control and processing of personal data. The GDPR serves as the cornerstone to the legal framework that protects privacy. However, while this might suggest that data protection is a subset of privacy, the right to data protection provides individuals with more rights over more types of data than the right to privacy (Lynskey, 2014).

2.4.3 The EU GDPR

Article 1 of the GDPR defines its goal. Paraphrased, it says, "this Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data" by laying down rules relating "to the processing of personal data and rules relating to the free movement of personal data" (EU, 2018b). It aims to give control back to the people the data refers to, to harmonise rules across countries to create a level playing field for business, and to enable the EU to enforce better, regulate and check compliance.

The GDPR sets out seven key principles: (i) Lawfulness, fairness and transparency; (ii) Purpose limitation; (iii) Data minimisation; (iv) Accuracy; (v) Storage limitation; (vi) Integrity and confidentiality (security); (vii) Accountability. The principles lie at the heart of the GDPR. They are set out right at the start of the legislation and inform everything that follows. They don't give hard and fast rules but rather embody the spirit of the general data protection regime, and as such, there are minimal exceptions.

Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative penalties. This could mean a fine of up to €20 million, or 4% of the total worldwide annual turnover, whichever is higher.

There are six available lawful bases for processing personal data. At least one of these must apply to process personal data: (a) Consent: the individual has given clear consent to process their personal data for a specific purpose. (b) Contract: the processing is necessary for a contract with the individual, or

because they have asked to take specific steps before entering into a contract. (c) Legal obligation: the processing is necessary to comply with the law (not including contractual obligations). (d) Vital interests: the processing is necessary to protect someone's life. (e) Public task: the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law. (f) Legitimate interests: the processing is necessary for legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if the entity is a public authority processing data to perform its official tasks.)

GDPR provides the following rights for individuals:

i Article 12-14 The right to be informed
ii Article 15 The right of access by the data subject
iii Article 16 The right to rectification
iv Article 17 The right to erasure
v Article 18 The right to restrict processing
vi Article 20 The right to data portability
vii Article 21 The right to object
viii Article 22 Rights in relation to automated decision making and profiling

The GDPR reflects the era in which it was drafted. In contrast to the 1995 Data Protection Directive, the GDPR incorporates terminology associated with the Internet (e.g., Internet, social networks, website, links, etc.). However, notable omissions include the term 'artificial intelligence' and related concepts like intelligent systems, autonomous systems, automated reasoning and inference, machine learning, or big data.

More recently, the EU has introduced or is planning to introduce five new relevant pieces of legislation that address some of the perceived shortcomings of the GDPR: the Data Markets Act (DMA) (EC, 2024a), the Data Services Act (DSA) (EC, 2024b), the Data Act (DA) (EC, 2023a), the Artificial Intelligence Act (AIA) (EC, 2023b) and the ePrivacy Regulation (EC, 2024c). The DMA governs competition and antitrust issues. So far, the EC has designated 6 dominant digital gatekeepers. The DSA governs consumer protection and safe online environments. So far, the EC has designated 17 very large online platforms (VLOPs) and 2 very large online search engines (VLOSEs). The DA governs fair access and user rights to data generated by Internet of Things (IoT) devices and related services. The AIA governs the safe and ethical use of AI systems within the EU and prohibits certain AI outright. It is expected to take effect in stages later in 2024. The ePrivacy Regulation (ePR) will replace the 2002 ePrivacy Directive that governs cookies and metadata. It will complement the GDPR's general rules on personal data processing by providing specific rules governing the privacy and confidentiality of electronic communications. While the ePR and the GDPR work hand in hand with each other, they both have different legal precedents. The ePR was intended to take effect before and then alongside the GDPR in 2018 but has been subject to repeated delays.

2.4.4 The US data protection regime

Constitutional data protection guarantees in the US are limited (Lawne, 2023; Parliament, 2015). US citizens may invoke protection through the Fourth

Amendment which states *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated"* (Madison, 1792). It, however, is not a guarantee against all searches and seizures, but only those that are deemed unreasonable under the law. The Constitution of the United States and the United States Bill of Rights do not explicitly contain a right to privacy per se. Instead, there is an implied right to privacy derived from penumbras of other explicitly stated constitutional protections (Cornell Law school, n.d.; US Supreme Court, 1965). In practice this means the data protection rights granted in the law are narrowly interpreted with a general tendency to privilege law enforcement and national security interests.

Unlike Europe, no singular federal law covers all types of data privacy (Klosowski, 2021). Instead, it has a patchwork of federal (and state) laws with acronyms like HIPAA, FCRA, FERPA, GLBA, ECPA, COPPA, and VPPA that tend to be more targeted in scope and contain a narrower set of obligations compared to the GDPR. These laws seek to protect personal data (known as Personally Identifiable Information (PII)) but not in as wide a manner as the GDPR (NIST, 2008). PII includes name, address, birth date, Social Security numbers and banking information, whereas the GDPR also references data such as photographs, social media posts, preferences and location as personal. The Privacy Act of 1974 protects PII but it only applies to certain federal agencies.

The Health Insurance Portability and Accountability Act (HIPAA) covers communication between a patient and "covered entities," which include doctors, hospitals, pharmacies, insurers, and other similar businesses. It does not cover all health data e.g. Fitbit data or vaccination status are not protected. The Fair Credit Reporting Act (FCRA) limits who can see a credit report, what the credit bureaus can collect, and how information is obtained. The Family Educational Rights and Privacy Act (FERPA) details who can request student education records. This includes giving parents, eligible students, and other schools the right to inspect education records maintained by a school.

The Gramm-Leach-Bliley Act (GLBA) requires consumer financial products, such as loan services or investment-advice services, to explain how they share data, as well as the customer's right to opt out. The law doesn't restrict how companies use the data they collect, as long as they disclose such usage beforehand. The Electronic Communications Privacy Act (ECPA) restricts government wiretaps on telephone calls and other electronic signals (though the USA Patriot Act redefined much of this). Critics point out that ECPA, which was passed in 1986, is outdated. Since ECPA was written well before the modern internet, it doesn't protect against modern surveillance tactics such as law enforcement access of older data stored on servers, in cloud storage documents, and in search queries.

The Children's Online Privacy Protection Rule (COPPA) imposes certain limits on a company's data collection for children under 13 years old. The Video Privacy Protection Act (VPPA) prevents the disclosure of VHS rental records. This law might sound silly now, but it came about after a journalist pulled the video-rental history of Supreme Court nominee Robert Bork. The Federal Trade Commission Act (FTC Act) empowers the FTC to go after an app or website that violates its own privacy policy.

At a state level, as with environmental regulation, California has led the way. The California Consumer Privacy Act (CCPA), introduced in 2020, shares many

similarities with the EU's GDPR. Eleven other states, including Virginia, Connecticut, Colorado, Utah, Iowa, Indiana, Tennessee, Oregon, Montana, Texas, and Delaware, had introduced similar legislation by the end of November 2023. Harkening back to the sub-section 2.3.3 on different regulatory approaches, the CCPA model leans more on consumers exercising their rights than documentation and governance compared to the GDPR.

In the absence of a comprehensive federal data protection or data privacy law, the aforementioned federal and state privacy-related laws are frequently the basis of class action lawsuits. While these laws offer protection for consumers, the nature of the alleged injuries — often intangible, future harms — has resulted in significant litigation as defendants challenge whether plaintiffs suffered an "injury" and have standing to bring their claims (IAPP, 2021). In theory, the cases should be easy to win especially when large-scale data breaches occur and a significant number of individuals are impacted. In practice, these cases have had mixed success. In a 2024 review of class action lawsuits, "less than 25% of the class certification decisions issued in data breach cases in 2023 came out in favour of plaintiffs" (Morris, 2024). In other words, the majority of courts decided against allowing the case to proceed as a class action. Nonetheless, privacy class actions continue to proliferate as plaintiffs search for new theories or angles of attack (Davis, 2024; Defense, 2025). Privacy and data breach class actions suits make up a fraction of the total number and value compared to securities class action suits but the trend is upward (Law, 2024; Rattigan, 2025).

The US system prefers self-regulation rather than big-state interference in the market economy. Big Tech has successfully argued that choice, transparency and self-regulation are preferable to the bureaucratic European model. Critics view this as a giant diversion. Consent and Notice have been the politicians' preferred solution to gain informed consent for decades. Matthew Crain (Crain, 2018), The limits of transparency: Data Brokers and commodification argues that data brokers appropriate transparency values in public relations to deflect the threat of government regulation. Transparency initiatives have created the illusion of reform while leaving the fundamental power imbalance intact.

In a world where data and the power to regulate its use are becoming central parts of statecraft, the United States is conspicuous in lacking a national data privacy law. Country-wide federal legislation relies on Capitol Hill, and the US Congress has simply been unable to pass an act with bipartisan support. The result is a patchwork of privacy protection legislation where the treatment of data transfers between states varies widely within the same country. US regulators are not unaware of this deficiency. Lina Khan, Chair of the Federal Trade Commission (FTC), is on the record as saying:

> *"When firms rely on business models that monetize personal data, it tends to create financial incentives to endlessly vacuum up people's sensitive information. As algorithmic decision-making tools further take hold, this data surveillance risks becoming even more entrenched. All too often, people must surrender to expansive tracking in order to use services that are essential for navigating modern life. Enforcing and strengthening laws against overcollection and misuse of our personal data is critical for maintaining people's right to privacy in the 21st century."* (Review, 2023)

Since her appointment in 2021, Lina Khan has attempted to tackle data abuses by treating them as a symptom of an underlying monopoly problem. However, this strategy has yet to prove its efficacy, as the FTC has faced setbacks in a series of high-profile antitrust lawsuits against Big Tech companies.

2.4.5 The Chinese data protection regime

In China, we see a third vastly different approach to privacy and antitrust in the digital economy. Emch (2019) argues privacy is not seen as such a cause célèbre compared to the West. There is not the same tension between the state and Big Tech because the government works closely with platforms and often views them as intermediaries to ensure compliance with approved policies. While platforms as regulators may have a negative connotation in the West, in China, he argues government actors perceive platforms as allies. Unless, that is, they get too big for their boots and Beijing calls their bluff as happened to Terry Gou, founder of Foxconn, in October 2023 when he boasted that he was untouchable and soon attracted the attention of tax inspectors (Hille, 2023). It evokes memories of how Beijing dressed down one of China's greatest entrepreneurs: Jack Ma, the founder of internet giant Alibaba. After Ma castigated the country's financial sector policies three years ago, regulators blocked the IPO of his fintech company Ant Group at the last minute (Zhu & Leng, 2020). The backlash forced Ma to retreat from his businesses and broadened into a campaign to discipline China's vibrant private sector.

Another internal dimension is control of the people. Data is used both as a control and feedback mechanism. It has been called Digital Leninism or Techno-authoritarianism. In "The Rise of Data Politics: Digital China and the World" (L. Liu, 2021), Liu argues that data has changed the basis of power. He asserts that a state's strength lies in not only its military or trading power but also its capacity to collect, refine, and utilise data, and its salience will only increase over time.

Two new Chinese laws dealing with data security and privacy came into force in November 2021, likely impacting many multinational companies operating in China or whose operations touch China. The Data Security Law (DSL) (Orrick, 2021; Translate, 2021) and the Personal Information Protection Law (PIPL) (National People's Congress (NPC) of the People's Republic of China, 2021) provide more specificity about the data localisation, data export and data protection requirements than first appeared in the Chinese Cybersecurity Law in 2017 (Peoples Republic of China, 2017).

The DSL sets up a framework that classifies data collected and stored in China based on its potential impact on Chinese national security and regulates its storage and transfer depending on the data's classification level. The law is generally seen as a response to the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (H.R.4943: 115th Congress (2017-2018), 2018), which gives US law enforcement agencies the authority to compel companies under US jurisdiction to produce requested data regardless of where the data is stored.

The PIPL is China's first comprehensive legislation regulating the protection of personal information and is modelled after the GDPR (Briefing, 2022). "Personal Information" is broadly defined as "any information related to identified or identifiable natural persons stored in electronic or any other format." However, personal information irreversibly anonymized is not covered (Skadden, 2021).

and the PIPL's definition of personal data does not include online identifiers, health, biometric, and genetic data, among other concepts (Interesse, 2023). Unlike the GDPR, the PIPL will be enforced by multiple regulatory bodies.

The PIPL generally applies to all types of data activities (e.g., collection, storage, usage, reorganisation, transmission, provision, disclosure and deletion) involving the personal information of data subjects in China, as well as activities outside China that are aimed at providing products or services to individuals in China or analysing their behaviour. Violations of the PIPL could face penalties of up to RMB 50 million (US$7.78 million), 5% of a company's annual revenue and disgorgement of all illegal gains.

2.4.6 Artificial Intelligence Act

The EU AI Act (EUR-Lex, 2024), approved by the European Parliament in March 2024, represents the world's first comprehensive AI regulation. Key prohibitions will start to come into force from August 2024. The interaction between the EU AI Act and GDPR presents emerging complexities in data governance. Both regulations overlap in addressing fairness, non-discrimination, and transparency in decision-making while requiring risk assessments for certain activities. However, gaps exist: the GDPR lacks explicit AI provisions, while the AI Act does not provide for a private right of action.

The GDPR establishes foundational principles for AI data usage, including data minimisation, purpose limitation and individual rights. The AI Act imposes stricter requirements for high-risk AI systems. Both address automated decision-making, with the GDPR offering specific individual safeguards. Organisations must navigate the applicability of each regulation based on their AI systems and data processing activities. While complementary, these regulations will likely require further clarification for consistent application.

Both regulations have significant financial penalties to incentivise compliance. The AI Act introduces a more nuanced approach to fines based on the risk level of the AI system and the nature of the violation. While the GDPR has hefty fines of up to 4% of global turnover, the EU AI Act raises the bar for high-risk AI breaches, potentially resulting in even steeper financial consequences (of up to 7% of global revenue). Until recently, GDPR regulators were criticised for not robustly enforcing their fining powers. It will be interesting to see if fines under the new AI Act will follow a similar timid trend or, conversely, possibly engender competition for bragging rights between the national GDPR regulators and the new central AI Office.

The AI Office, a new division within the European Commission, is tasked with drafting secondary laws that set out how the primary legislation principles should be applied in practice. However, the AI Act does not specify clearly which agency at a national level should police the rules. It remains open whether local telecoms, competition or data protection authorities will eventually implement it nationally (Espinoza, 2021).

In summary, the new AI Act may strengthen data protection by closing loopholes, but it will also create new complexities in its interaction with the enforcement of the GDPR.

2.5 Summary

Privacy is a concept that has evolved over time due to changes in technology and social norms. While there is a global consensus on the need for digital privacy protection, there is no singular agreed-upon definition of privacy. The data economy is a global digital ecosystem in which data is gathered, organized, and exchanged by a network of companies, individuals, and institutions to create economic value. Surveillance capitalism is a concept in political economics which denotes the widespread collection and commodification of personal data by corporations. This phenomenon is distinct from government surveillance, although the two can be mutually reinforcing. Regulation in theory is designed to correct market failures and information asymmetries. To make the nebulous concept of privacy more tractable, data regulation focuses on the processing and transferring of personal data. The U.S. relies on market self-regulation, China trusts the state, and Europe employs arms-length regulators. The enforcement approaches also differ, with the U.S. favouring notice and consent while China and Europe adopt more prescriptive measures. Building upon the content in this chapter as context, Chapter 3 reviews the scholarly literature that motivates the research aims and investigations undertaken in the ensuing four chapters.

Chapter 3

Literature review

In this Chapter, I review the literature that analyses the concept of success or achieving a successful outcome within the context of the GDPR. It examines measures of success from the perspectives of three different but involved stakeholders: business, informed individuals, and GDPR regulators. It also looks at the literature on the known challenges, limitations, and wish lists related to the GDPR's future shape. We will show there is: 1. little in the way of documented concrete business benefits, 2. a scarcity of research into whether employees who have experienced the GDPR implementation think it was worth it or not, 3. an absence of means to assess regulator performance per se and the comparative performance of regulators across the EU, and 4. a reluctance by commentators to synthesise their insights into a cohesive picture of the GDPR's future trajectory. The review concludes by demonstrating how these gaps identified in the literature informed the empirical work in this thesis.

3.1 Business benefits

The literature review of the GDPR's benefits to business has two parts: non-academic and academic. First, we review coverage by the EU and the advisory industry, and second, we review coverage by academia. In both cases, there is a clear gap in the GDPR assessment from a business perspective.

3.1.1 GDPR objectives & obligations

To recap, the GDPR came into force on 25 May 2018 (European Parliament and of the Council, 2016), after which all organisations were required to comply. The UK GDPR, post-Brexit, was ruled as adequate by the EU in June 2021. Unlike its predecessor, the GDPR is an EU Regulation and not a Directive. This means it has binding force in every member state, and there is no discretion over how it is transposed into national law.

The primary purpose of GDPR is to define standardised data protection laws for all member countries across the European Union. In summary (European Union, 2022), it was intended to:

- Increase privacy and extend data rights for EU residents.
- Help EU residents understand personal data use.

- Address the export of personal data outside of the EU.
- Give regulatory authorities greater powers to take action against organisations that breach the new data protection regulations.
- Simplify the regulatory environment for international business by unifying data protection regulations within the European Union (a.k.a. the level playing field).
- Require every new business process that uses personal data to abide by the GDPR data protection regulations and Privacy by Design rule.

It has strict rules such as the rights for data subjects to access their own data (known as SARs), to be forgotten and to expect affirmative consent. It applies to companies inside and outside the EU if they hold personal data belonging to EU citizens. And it has tight data breach notification requirements and hefty fines of up to four percent of an organisation's total worldwide annual turnover if found in violation (GDPR.eu, 2018).

GDPR is strong on the obligations of business. It makes no reference to any benefits to business.

3.1.2 GDPR scorecard

The EU has commissioned a number of surveys since the GDPR was applied. We highlight three surveys here: the 2019 Eurobarometer, the 2019 SME Survey and the 2020 EU Self-Evaluation Report.

The 2019 EU Barometer 487a found that:

- Over 66% of EU citizens have heard of GDPR, over 50% have heard of their rights under GDPR, and almost 60% have heard of their data regulator.
- A majority feel they have partial control over the information they provide online. Only 20% say they see the Terms & Conditions (T&C's) to the collection and use of their personal data online, and only 13% say they read privacy statements in full.

The 2019 GDPR Small Business Survey was run by Proton Technologies AG. Part-funded by an EU Horizon Project, it found:

- Millions of small businesses still do not comply with the GDPR.
- Encryption technology is still not widely understood.
- Small businesses want to comply and have invested heavily on GDPR compliance.

On June 24, 2020, the European Commission (EC) submitted its first report on the evaluation and review of the GDPR to the European Parliament (EP) and Council. The report is required under Article 97 of the GDPR and will be produced at four-year intervals going forward. In its report, the Commission concludes that generally the GDPR has successfully met its objectives, namely those of strengthening personal data protection and guaranteeing the free flow of personal data within the EU. It identified a number of areas for improvement, including:

- Fragmentation between member states: differential interpretation of discretionary details

- Uneven enforcement: different *"data protection cultures"*, different budgets & resources
- Unforeseen Issues with Emerging Technologies: AI, IoT or facial recognition
- Unused Potential of Data Portability Rights: to avoid unfair practices and lock-in effects
- Adequacy Decisions: Pending third country regimes such as South Korea and UK
- Extra-territorial Reach: *"This approach should be pursued more vigorously in order to send a clear message that the lack of an establishment in the EU does not relieve foreign operators of their responsibilities under the GDPR."*

Whilst this report is akin to the EC marking its own homework and not an impartial external assessment, it is still a useful checklist of where the EC sees shortcomings in GDPR.

3.1.3 Gap in GDPR scorecard

Our search has revealed a significant gap in the assessment of GDPR. There seems to be no equivalent to the EC's four-yearly evaluation and review from the perspective of one important stakeholder: the regulated businesses that handle customer data.

In the run-up to GDPR going live in 2018, there was a flood of surveys, studies and benchmarking reports by IT vendors and professional services firms. Since then, they have dried up.

One exception is the EU Multistakeholder Expert Group. Set up in 2017, it assists with identifying the potential challenges in the application of the GDPR from the perspective of different stakeholders, and to contribute to the EC's evaluation of GDPR in 2020. It is composed of up to 27 members drawn from trade and business associations, NGO's, academics, legal practitioners and privacy advocates. It is quite technocratic. Their *"contribution addressed topics such as the impact of the GDPR on data subjects' rights, the conditions for a valid consent under Article 7(4) of the GDPR, the one-stop-shop mechanism, the principle of accountability and the risk-based approach, data protection officers' ('DPOs'), the relationship between controllers and processors, and the development of Standard Contractual Clauses for the transfer of personal data"* (European Commission, Directorate General for Justice and Consumers, 2020). Benefits analysis is not part of its mandate.

One of the few non-EU follow up surveys was a survey by Deloitte's *"A new era for privacy: GDPR six months on"* (Deloitte, 2018). The headline was that consumer awareness has risen and 48% of organisations had made "significant" investment to improve their compliance. In addition:

- 70% of organisations had increased staff focused on GDPR compliance.
- 92% of organisations claimed confidence in their ability to comply with GDPR in the long term. 65% of organisations felt they had enough resources to comply.
- 78% had invested in new data loss prevention and 71% in unstructured data scanning.

Another non-EU study is the annual implementation progress report that is published by Access Now, a digital rights group. In their latest, *"Three Years Under The EU GDPR"* (Masse, 2021), they describe GDPR as *"nothing but hot air"* because of slow and weak enforcement by the Data Protection Authorities (DPA). The EU is criticised for under-resourcing its DPAs and failing to levy sufficient fines and sanctions on business. This presents the EU and its DPAs with a media communications challenge - satisfying consumer rights protection groups and, at the same time, selling the benefits of a level playing field and GDPR compliance to business.

3.1.4 Academic literature

There is no shortage of academic GDPR studies. A Google Scholar search of the General Data Protection Regulation will yield close to 4 million hits. Limit the search to papers published after GDPR went live in 2018 however and interest drops precipitously. Search for papers that contain the two keywords "GDPR success" or "GDPR benefits" anywhere in the text yields less again. As I narrowed the search, I quickly reached zero hits for keyword combinations such as "GDPR business benefits" or "GDPR consumer benefits" or even "benefits of GDPR to business". The lack of curiosity about GDPR's benefits to business after 2018 is curious.

In the following sections, I review the plentiful literature on the implementation challenges of GDPR. I examine papers that contained the word pair "GDPR success" and "GDPR benefits" anywhere in their text as well any relevant papers from multiple rounds of backward and forward searches. Most do not address directly this concept because they are not interested in how GDPR might deliver value or return from a business perspective. The studies in Section 3.1.6 explore exclusively regulatory angles. Other papers discussing benefits in fact only consider drawbacks (Section 3.1.7).

The two papers (Almeida Teixeira et al., 2019; Poritskiy et al., 2019b) that do explore positive aspects of GDPR to businesses rely mainly on pre-GDPR work. We conclude that given the newness of GDPR, there are still few scientific follow-up studies.

3.1.5 Studies on implementation challenges

Unlike benefits, there is a surfeit of studies on the challenges of GDPR. It is a complex regulation (Freitas & Mira da Silva, 2018), it fails to specify technical solutions (Tikkinen-Piri et al., 2018) and it involves subjectivity (Agarwal, 2016). Compliance can be expensive (Addis & Kutar, 2018; Tikkinen-Piri et al., 2018). Companies may need extra administration staff and expert DPO staff (Lindgren, 2016), extra employee training and face difficulty recruiting and retaining these people (Khan, 2018). Regulatory restrictions may impact an organisations performance (van der Marel et al., 2016) and persuade some to cut back their service offering in the EU to avoid it (Allen et al., 2019).

GDPR brings increased technical complexity (Bennett, 2018; Dubrova, 2018; Politou et al., 2018). Data portability (Kaushik, 2018) as well data consent, rectification and deletion processes will require technical and organisational investment (Dubrova, 2018). Data erasure (aka the right to be forgotten) is seen as particularly problematic for larger companies (De Hert et al., 2018; Dove,

2018). System and process audits (Dubrova, 2018) and recruiting more cybersecurity professionals will require more investment. Clamping down on how personal data is handled may slow down the development and application of emerging technologies such as IoT and blockchain (Li et al., 2019; Wallace & Castro, 2018).

3.1.6 Studies on GDPR success

Unlike challenges, there is a dearth of research on success. Under "GDPR success", the most relevant literature has a regulator or regulatory success focus rather than any reference to business success. Thus, Oxford Analytica's appraisal of GDPR on its first anniversary (2019) looked at key shortcomings such as ensuring the compliance of business beyond "big tech", concern that public awareness of the GDPR in smaller EU states will lag that in larger states and criticism of the Irish regulator if it failed to demonstrate a clearer commitment towards robust regulation. Sanders, in *"The GDPR One Year Later"* (2018) suggests the key to the GDPR's success requires data protection officials and judges to seriously evaluate situations in which privacy and freedom of the press appear to conflict. Kessler in *"Data Protection in the Wake of the GDPR: California's Solution for Protecting 'the World's Most Valuable Resource'"* (2019) argues that the United States should adopt a federal standard that offers consumers similarly strong protections as the GDPR.

3.1.7 Studies on GDPR drawbacks

Despite searching for "GDPR benefits", the literature is about the dis-benefits of GDPR, albeit with more of a focus on businesses. *"The Economic Impact of the European Reform of Data Protection"* is a (2015) paper by M Ciriani of the Regulatory Office of the French mobile phone operator, Orange. She argued that the extraterritorial application of European law would promote a level playing field within the European market. However, with the exception of the GDPR's impact assessment conducted by the European Commission, she claimed the literature she had examined shows that the costs of GDPR's adoption might offset the efficiency gains. She expressed concern that increasing the administrative burden might not help improve the competitiveness of European digital service providers, such as her employer. Flexible ex-post effects-based accountability would help industry.

Sarah Shyy, in the self-explanatory *"The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business"* (2020) argues that GDPR fails to promote consumer privacy because, in today's data collection practices, consumers are forced to accept an online company's privacy policy and data collection practices. Meanwhile, the GDPR has disadvantaged SMEs by imposing cost-prohibitive measures, hindering SMEs growth, and spurring SMEs to exit the market. Rather than copying the GDPR model, she argues US lawmakers should learn from the GDPR's failings and adopt regulation that is both more effective in protecting consumer privacy and less burdensome on businesses.

3.1.8 Studies on GDPR benefits to business

There are two academic papers (Almeida Teixeira et al., 2019; Poritskiy et al., 2019b), published in 2019, that are relevant from a business perspective.

Poritskiy et al. ask what are the main benefits offered by GDPR for IT companies (2019b). They surveyed 286 Portuguese IT companies that were partners of their educational institution on eight benefits (and nine challenges) drawn from a literature review. On closer reading, the benefits stem from opinion pieces that pre-date the introduction of GDPR rather than empirical research.

They concluded the two most significant benefits were trust (consumer confidence) and legal clarification. These two benefits chime with two of their sources, Bilyk (2018) and White (2018). The Bilyk study references a blog on theappsolutions.com website credited to a different author and the White study appears to reference a (now) broken link to a GDPR news report. Another two of the eight benefits of GDPR, better decision-making and better risk-assessment, are also credited to Bilyk. Two more of the eight benefits, increased security of products / services and increased quality of documentation, are credited to Krikke et al. (2019) which appear to reference brochure-style content on the site of the law firm Stibbe.com. Another benefit, create new competitive advantages, is credited to Dellie (2019) which references a blog on the ITASCA.org site. Two further benefits, minimisation of the collected personal data and improved data management processes, are credited to Fimin (2018) which references an article in Forbes magazine by the CEO of cybersecurity firm. The eight benefits surveyed in the questionnaire may indeed be real but the cited evidence behind them is not based on any qualitative or quantitative data.

In the second paper, Teixeira et al. (2019) conducted a systematic literature review to identify the critical success factors that contribute to the implementation of GDPR. One of the research questions was *"What are the benefits of complying with GDPR?"*

Their review identified four potential areas of benefit: proper data management, use of data analytics, cost reduction and an increase in reputation and competitiveness.

Regarding data management, Lopes and Oliveira view GDPR as an opportunity for companies to document their processes and procedures (2018). Presthus et al. sees it as an opportunity to cleanse and audit personal data to cap any liability to abuse of personal data (Presthus et al., 2018) and similarly, Skendžić et al. view GDPR as an opportunity to bring data consistency across the organisation (2018).

Better data management enables better data analytics. Garber argue data-driven insights will help inform companies optimise their business processes and identify new business development opportunities (2018). Enhanced data management will lower costs by eliminating surplus data, redundant data and, thus, data storage costs (Beckett, 2017; Miglicco, 2018; Perry, 2019). O'Brien reports it could reduce costs by up to 2.3B EUR per annum according to estimates by the European Commission (2016). Beckett postulates that GDPR compliance and safe data governance skills may enhance a company's trustworthiness and generate new business and new customers (2017). Tikkinen-Piri et al. argue the adoption of GDPR may give a competitive advantage to organisations (2018). Garber (2018) and Miglicco (2018) believe compliance may also boost an organ-

isations' performance by improving operational efficiency.

The first paper (Poritskiy et al., 2019b) is a quantitative survey of GDPR dimensions based mainly on pre-GDPR literature. The second (Almeida Teixeira et al., 2019) is a systematic review of historic literature regarding GDPR success factors. Both look to the future and talk in terms of potential barriers and enablers. The former admits it does not explore implementation challenges nor company specifics and the latter admits it is unable to identify or present practical outcomes.

3.1.9 Motivation summary

Given that GDPR is a relatively recent regulation, few scientific follow-up studies exist. Neither of the two 2019 papers (Almeida Teixeira et al., 2019; Poritskiy et al., 2019b) nor the review here could identify or substantiate specific benefits to business of implementing GDPR. Hence, in Chapter 4, we present research we conducted with business executives on the perceived benefits of the GDPR and how those effects are felt within and across their organisations.

3.2 Consumer/Employee perceptions

People who were employed before May 2018 and who are still employed by the same organisation will have experienced the impact of the GDPR on their workplace firsthand. They both implement it as employees and benefit from it as consumers. The goal of this study is to understand the unique dual perspective of this group. Given the unique nature of our research target group, we review the literature from multiple perspectives—namely, consumer awareness and knowledge of the GDPR and DPAs, consumer perceptions of privacy, the response of business to implementing the GDPR, the awareness of staff within the business of the measures required to operationalise it and their perception of its benefit to them and to their company. We find outstanding contradictions in prior works and blind spots that lead us to a series of research questions that we investigate further in our study as summarised in Section 3.2.7.

3.2.1 Consumer awareness and knowledge of the regulation

An informed citizenry is vital for a well-functioning democracy. The GDPR makes the awareness-raising duties of Data Protection Authorities (DPA) explicit. Under Article 57.1, the DPAs have an obligation to *"promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing*". DPAs employ various activities to raise awareness, ranging from publishing press releases, penalty notices, educational materials and commentaries, to hosting public meetings and events. These activities are aimed at companies as much as at citizens (Jasmontaitė-Zaniewicz et al., 2021).

The success of this awareness-raising challenge attracts wildly differing verdicts. On the low side, a private survey of over 289K consumers, coinciding with the first anniversary of the GDPR on May 2019, found *"A staggering eight percent of consumers globally feel they have a better understanding of how companies use their data since the GDPR's introduction*" (PR Newswire, 2019).

On the high side, a Eurobarometer survey on the same May 2019 anniversary found 67% of respondents had heard of the GDPR, 36% had heard of it and knew what it was, almost 73% had heard of at least one right guaranteed by the GDPR and 31% had heard of all the rights asked about in the survey (European Commission. Directorate General for Justice and Consumers. & Kantar., 2019). The level of awareness varied wildly between countries, from 90% in Sweden all the way to 44% in France.

A later secondary analysis of the same 2019 EU Eurobarometer survey showed education, occupation, and age were the strongest socio-demographic predictors of the GDPR awareness, with little influence of gender, subjective economic well-being, or locality size.

Sources of information also differ. In the 2020 *"Data Protection or Data Frustration? Individual Perceptions and Attitudes towards the GDPR*", Strycharz et al. found most respondents learnt about the Regulation from the news (47%), followed by their employer (36%) and cookie notices on websites (2020).

Despite the contradictory results from prior surveys, we hypothesise that the trend is positive and that consumers are aware of and knowledgeable about the GDPR.

3.2.2 Consumer awareness and knowledge of the regulator

Conscious of their duty to promote public awareness, regulators conduct surveys, albeit their definitions and metrics vary wildly across the EU. Professional services firms and data rights groups also conduct and publish GDPR-related surveys. Academic surveys on regulator awareness are sparse.

An EU Eurobarometer survey (European Commission. Directorate General for Justice and Consumers. & Kantar., 2019) of 27,524 people across the 28 member states found 57% had heard about the existence of a public authority in their country responsible for protecting their rights regarding their personal data—an increase of 20% on a 2015 survey.

The Belgian DPA takes a different approach. In its 2020 annual report, it congratulates the increased awareness of citizens because *"the year 2020 saw a sharp increase in the number of complaints (+290.64%) and data breach notifications (+25.09%) received by the BE DPA and, more generally, a significant increase in the DPA's workload*" (2021).

The UK Information Commissioner's (ICO) 2021 Annual Report contains an annual track survey of 2,000 people to measure its strategic performance in supporting the public. It found 28% of people have high trust and confidence (compared with 27% in 2020), with a similar number state they have low trust and confidence (29%, compared with 28% in 2020) (2021).

Awareness of the GDPR translates for some into awareness of the regulator's punitive power. For example, the international law firm DLA Piper (2022) publishes an annual fine and data breach survey as part of their public relations strategy to communicate the need for proper advice on GDPR matters. Privacy advocates follow a similar path. AccessNow (Masse, 2021) is a digital rights group that publishes an annual evaluation of GDPR. In its most recent report 'Three Years Under GDPR', it focuses on the number and value of data fines and concludes 'GDPR implementation is proving to be nothing but hot air' due to a lack of enforcement.

In sum, apart from the EC's four-yearly survey, regulators are not measuring their brand awareness. Instead they measure proxies such as customer confidence, consumer complaints or breach notifications whilst professional services firms and advocacy groups focus more on fines for their own reasons. Familiarity with the regulator among laypeople appears to be under or untested. We hypothesise that consumers lack awareness and knowledge of their regulator.

3.2.3 Consumer perceptions of privacy

Side-stepping the privacy-paradox debate and whether privacy desires and privacy actions are consistent, we are interested in how people feel or perceive the state of their privacy post-GDPR. We find contradictory studies that claim it has had little impact, and others believe it has improved people's feeling of privacy.

In 'Are consumers concerned about privacy?', conducted in the run-up to GDPR, Presthus and Sørum found the respondents had a favourable view of the GDPR, but they were sceptical about its enforcement (2019). In a follow-up, 'A three-year study of the GDPR and the consumer', they found that the GDPR has not significantly affected consumer awareness nor the level of control over their own personal data (2021).

There is some evidence that consumer perceptions of power and risk in digital information privacy have risen due to mandatory the GDPR cookie notices (Bornschein et al., 2020). In a similar vein Zhang et al. (2020) suggest that the GDPR plays a significant role in online customer trust by bringing about stronger rights and more transparency for online customers.

A 2021 survey by the ICO (Worledge & Bamford, 2021) found that 77% of people say protecting their personal information is essential. The survey does not ask about privacy per se. Instead, it asked 'Has your trust and confidence in companies and organisations storing and using your personal information increased, decreased or stayed the same in the past year?', they found 9% felt it had increased, 68% felt it had stayed the same and 23% felt it had decreased compared to 2020. The answers in percentages were broadly the same as the 2020 survey results. Given the unique perspective of our sample, we believe that it is apposite to seek their evaluation of the effect of the GDPR on their privacy perceptions. We hypothesise that consumers feel their privacy is better since the GDPR was introduced.

3.2.4 Business response to Data Protection regulation

To comply with the GDPR, most companies will have had to make some legal, technical and organisational changes (Poritskiy et al., 2019a). Failure to comply can attract hefty fines of up to 4% of global turnover (GDPR.eu, 2018) and negative publicity which in turn can affect a company's market valuation if it is publicly quoted.

A systematic literature review (Spanos & Angelis, 2016) into the economic consequences of security incidents found that most studies (76%) report a statistically significant negative impact of data breach events on the stock market. Ford et al. (2021) found cumulative abnormal returns of around -1% after three days far outweighed the monetary value of the fine itself, and relatively minor

fines could result in major market valuation losses for companies. The persistence of this effect is open to debate and Richardson, Smith and Watson argue that 'companies are unlikely to change their investment patterns unless the cost of breaches increases dramatically or regulatory bodies enforce change' (2019).

In one of my earlier papers (Buckley et al., 2022) and described as part of this thesis in Chapter 4, I found the fear of the GDPR's threat of meaningful financial penalties has spurred companies to take the GDPR seriously. It has led to modernisation of company databases, more careful accounting of data, and greater awareness of information security. Cochrane et al. (2020) and Jasmontaitė-Zaniewicz et al. (2021) surveyed SME Associations and found evidence to support Hijmans' (2018) view that information and awareness of the imposition of fines was a regularly cited way of capturing the attention of SMEs.

Thus GDPR compliance, whatever the corporate motivation, should have been and continue to be a visible agenda item for employees in almost all company departments (ICO, 2018b). People in Finance and IT would be aware of the cost of additional IT information security expenditure and the potential size of fines. Staff in Human Resources and Customer Service would be aware of personal data handling requirements and subject access requests. Executives in Sales and Marketing would be aware of purpose limitations and the need to gain consent to promotional campaigns. We are interested in testing this commitment since public statements of investment and compliance are cheap. We hypothesise that companies have responded to the GDPR and made changes.

3.2.5 Employee awareness of their employer's Data Protection regulator

It is reasonable to assume the in-house Data Protection Officer (DPO) will know the identity of their DPA since they will be required to communicate with it. However it is less clear if staff, in general, know their DPA and even more so if the DPO function is outsourced to an external provider, which is quite a common business practice for SMEs (Dataguard, 2022).

Under article 57.1 (Intersoft Consulting, 2018), DPAs also have a duty to engage in activities furthering 'the awareness of controllers and processors of their obligations', i.e. the individuals and companies that handle personal data. Making companies aware of their responsibilities would seem obvious if they are expected to be held accountable for their actions. However, it is also the nexus of the two schools of enforcement which are (punitive) deterrence or (advisory) compliance.

Hodges (2018) asserts that DPA awareness is essential if it is to play a leadership role where the emphasis is on the expertise, authority and influence of the DPA. Hijmans (2018) partly agrees but argues that for enforcement of the regulatory framework to be successful, regulators should have sufficient resources and capability to issue strong sanctions. The GDPR includes both compliance and deterrence approaches.

Data on employee awareness of their employer's GDPR regulator is inconclusive. Deloitte, the management consultancy, Deloitte (2018) found 57% of respondents indicated their organisations had received regulatory requests from their DPA. Later in the same year, STAR delivered a report to the EU that found *"Most DPAs neither conduct specific research aimed at establishing levels*

of SME awareness nor general awareness of the GDPR" (Barnard-Wills et al., 2019).

If companies have invested in training, then employees should be familiar with at least the name of their company's regulator and with the size of the fines their company could face. However, given the uncertainty, we hypothesise that employees lack awareness of the GDPR regulator at work.

3.2.6 Employee perception of benefit of the GDPR to their employer

Literature on the benefits of the GDPR to business is somewhat limited. Studies focus on the technical, financial and human resources struggles that companies encounter in complying with the regulation (Tikkinen-Piri et al., 2018). Training employees is challenging, including even data scientists. Larsson and Lilja (2019) argue that the GDPR will provide some opportunities for other businesses, like legal experts, lawyers, consultants in digital strategy and professionals in analytics. Poritskiy et al. (2019a) find the main benefits identified include increased confidence and legal clarification whilst the main challenges include the execution of audits to systems and processes and the application of the right to erasure.

Almeida Teixeira et al. (2019), in their systematic literature review, find the literature reflects on benefits that organisations may achieve by implementing the GDPR including proper data management; use of data analytics; cost reduction; and increase in reputation and competitiveness. This review was conducted in 2019 and looked back at literature that is pre-GDPR mainly in practice.

More recently, my work as outlined in the next Chapter 4 looked at the actual impact of the GDPR on companies after three years. It found that the GDPR had made companies more privacy-aware, spurred modernisation of their data processes and justified upgrade investments to their security infrastructure. At the same time, it found evidence that it had made new business development harder due to restrictions on requesting and holding personal data, increased direct and indirect compliance costs, left companies confused at times due to grey areas of law and exposed companies to burdensome subject access requests.

Many of these benefits and complications may be invisible or above the pay grade of employees, which is why we hypothesise that employees have seen little benefit to their company from GDPR.

3.2.7 Motivation summary

Westin's work on different attitudes to privacy (Kumaraguru & Cranor, 2005) and, Acquisti's studies (2005; 2013, 2015, 2016) on the economics of privacy help us to begin to understand how individuals rationalise the importance and effort they treat protecting their data. People instinctively know there are trade-offs.

With the shift to the internet and the datafication of society, it has created what Shoshanna Zuboff describes as *"a wholly new subspecies of capitalism in which profit drove from the unilateral surveillance and modification of human behaviour*" (2019b). Policymakers have struggled with finding the right balance between competing interests and the GDPR is their latest attempt at squaring the circle. The purpose of the GDPR is to protect individuals and the data

that describes them and to ensure the organisations that collect that data act responsibly.

The literature review has revealed six hypotheses for study:

1. Consumers are aware and knowledgeable about the GDPR.
2. Consumers lack awareness and knowledge about the regulator.
3. Consumers feel their privacy is better since GDPR was introduced.
4. Companies have responded to GDPR and made changes.
5. Employees lack awareness of the GDPR regulator at work.
6. Employees have seen little benefits to their company from GDPR.

In Chapter 5, we investigate these six hypotheses and seek to answer the key research question: *"do you think it is worth it?"*

3.3 Regulator Performance

Regulation studies is a vast field encompassing political science, economics, law, sociology and psychology. Our focus is on the effectiveness of privacy regulators. Since we covered the importance of regulation, its logic, and how it is administered in the Background Chapter 2, we have edited down the literature review from the original paper to include only additional key contextual information. In particular, we tease out how the theory maps to the everyday implementation of the GDPR. We show that weak performance measurement of regulators is a common issue and is especially lacking in the case of data protection regulators. We draw inspiration from management theory on scorecard frameworks to address this systemic blindspot.

3.3.1 The practice of Data Protection regulation

There are three broad modes of regulation (Coglianese & Lazer, 2003): technology-based, which is prescriptive and often has strict auditable standards; management-based, where business design their own compliance plan but where the capacity to assess it externally is difficult; and incentive or performance-based, where business design their own plan and where it can be assessed externally against regulatory targets.

The GDPR is a mix of the three modes of regulation but not in equal measure. Two NGOs interviewed in this chapter say they want it to be more technology-based and issue fines for clear-cut violations like automated speeding tickets. Others want it to be more performance-based, but it is difficult to assess a company's privacy practices without entering their premises and observing them in detail. As a result, the GDPR is mostly management-based, with companies committing to implementing the appropriate people, processes, and technology to support compliance.

The theory of enforcement broadly splits along hard and soft lines (Abbott & Snidal, 2000). Hard Deterrence (or Command and Control) enforcement assumes businesses will try to evade regulations. It tends to be rules-based and a companion to the technology-based mode of regulation. Soft Persuasive (or Co-operative) enforcement assumes business will try to comply. It tends to be more principles or risk-based and a companion to management or performance-based mode of regulation. Gaming studies (Potoski & Prakash, 2004) suggest the

cooperative approach improves the chances of low-cost compliance in the long run. If a firm evades, the government can use enforcement, "tit for tat" (Scholz, 1984), or it can employ "responsive regulation" (Ayres & Braithwaite, 1992), otherwise known as the "walk softly and carry many sticks". Critics (Abbott & Snidal, 2013) question this since it assumes the regulator has perfect information, perfect discretion, knows the right proportionate response, suffers no turf wars and can credibly commit to using the strongest enforcement mechanism when necessary.

Enforcement of GDPR is a mixture of hard and soft regulation. The powers delegated to regulators are awe-inspiring, including the power to fine a company up to 4% of global revenue and/or the power to ban a company from processing certain data which could bring a company's operations to a halt. Whereas enforcement theorists stress a coercive strategy of monitoring and sanctions, management theorists embrace a problem-solving approach based on capacity building, rule interpretation, and transparency. Research suggests that enforcement and management mechanisms are most effective when combined in a "management-enforcement ladder" (Tallberg, 2002). Typically it escalates from (i) rule publicity to avoid inadvertent non-compliance (ii) enhanced monitoring (iii) legal proceedings and/or bargaining with violators (iv) sanctions or fines if non-compliance persists. As we shall see, regulators differ in how they interpret and exercise their powers.

Compliance is driven by external and internal influences that generate its "social license" (Gunningham et al., 2004). External pressure may come from company shareholders, NGOs and customers. These actors, in effect, give companies their "social license to operate," and pressure can revoke that license. Internal pressure may come from the employees in trust and management-based regulation. Compliance requires buy-in from the company and is related to deep commitment, routinization, professionalization (Barnes & Burke, 2012). This is why naming and shaming can sometimes be effective.

3.3.2 The role of a regulator

We examine why we delegate authority to bureaucracies and how we hold them accountable whilst protecting their independence.

Governments delegate authority to bureaucracies for two reasons: competence and credible commitment (Gilardi, 2002). Bureaucracies have expertise that politicians lack, especially in complex policy and technological areas. This expertise can help reduce transaction costs and resolve disputes. Governments can also delegate authority to bureaucracies to tie their own hands and commit to stable policies. This can help prevent governments from taking expedient short-term measures that may be harmful in the long run (Keefer & Stasavage, 2002; William Bernhard, 1998). To insulate senior officials from political interference, governments typically give them fixed terms of tenure, allow them to be fired only for cause, and remove them from direct executive control.

This independence can create its own issue, namely the principal-agent problem, where the agent (the bureaucracy) has more knowledge or policy expertise than the principal (the politicians) and can shirk or deviate from the principal's wishes. To mitigate this problem, governments can give agencies less authority when the issue is salient to the public (Bawn, 1997; Gormley, 1986; Randall L. Calvert et al., 1989; Spence, 1997) and more authority when the issue is com-

plex and requires expertise (Bawn, 1995). Governments can also put in place monitoring agencies, administrative procedures, and policy evaluation tools to check on agencies and reduce the potential for bureaucratic drift.

De facto independence, or the ability of a bureaucracy to act without political interference, is achieved through a good reputation and autonomy (D. P. Carpenter & Krause, 2012). A good reputation is built on a history of competence, consistency, and flexibility. Autonomy is granted when "political authorities see it as in their interest to defer to agency action" (D. Carpenter, 2001). Together, these factors can protect a bureaucracy from political threats and meddling.

3.3.3 The role of the GDPR regulator

We examine the regulatory architecture behind the GDPR regulator and the light-touch accountability.

The EU has its own legislature (the European Parliament and the Council of Ministers) and executive (the European Commission (EC) and the European Council), as well as an independent judiciary and a central bank. These are supported and complemented by a set of institutions and bodies, including inter alia the European Ombudsman (EO), the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS).

The EDPB (EU, 2018g) is *"an independent body of the Union"* (recital 139) with legal personality that contributes to the consistent application of data protection rules throughout the European Union and promotes cooperation between supervisory authorities. The EDPB comprises the heads of the supervisory authorities (SA) and the EDPS, which provides secretariat services. It can provide general guidance (including guidelines, opinions, recommendations and best practices), advise the EC on new proposed legislation relating to data protection, make binding decisions addressed to the supervisory authorities in member states, and promote cooperation and the effective exchange of information and best practice between them (European Data Protection Board, 2023). The EC has the right to participate in the activities and meetings of the Board without voting rights. The Chair of the EDPB communicates to the EC the activities of the EDPB.

The Supervisory Authorities (A.K.A the DPAs) are the national data protection regulators. Each member state must appoint one (or more) (EU, 2018c), and they must be independent (EU, 2018c) and "free from external influence." Member states are required to furnish them with adequate human, technical and financial resources, premises and infrastructure necessary for the effective performance of their tasks and exercise of their powers. Member States are required to appoint staff by means of a transparent procedure (by their parliament, government, head of State, or an independent body), for a fixed term only dismissable in cases of serious misconduct.

Regarding national oversight, each member state must ensure that each SA is subject to financial control, which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget. In terms of European oversight, the GDPR has very little to say other than Article 59 (EU, 2018f) and Activity Reports *"Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2) (EU, 2018e). Those reports shall be transmitted to*

the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and the Board." Accountability is defined in three sentences.

3.3.4 Regulator performance assessment

According to the OECD Best Practice Principles on the Governance of Regulators, a well-designed performance framework serves multiple goals: demonstrating the effectiveness of the regulator, building confidence in the regulatory system and driving improvements (OECD, 2011). Performance assessment is a critical ingredient for maintaining accountability and fostering transparency, and public bodies are often required to report on results and enable scrutiny of their performance. Data on the performance of both the regulator and the regulated sector are an important ingredient of economic regulators' performance assessment frameworks. The results can also be part of organisational learning, providing inputs into decision-making.

The theory of performance assessment of regulators has evolved. Early approaches focused on compliance monitoring. Ogus (2004) identified the shift from command and control to more flexible and performance-based approaches that incentivize industries to improve their performance. Output-based regulation (Joskow & Rose, 1989) focuses on regulating outputs rather than inputs, while outcome-based regulation (Hahn & Dudley, 2004) sets specific, measurable goals for the industry and evaluates their progress towards these goals. Risk-based regulation (Baldwin et al., 2012) assesses the likelihood and potential impact of risks associated with complex industries with significant uncertainty. Contemporary scholars such as Coglianese (2012) argue regulatory performance should be measured by evaluating the impact of regulation and regulatory policy on society, including how well regulations achieve their intended goals, how much they cost, and how they affect different groups of people.

In recent years, governments like the UK (National Audit Office, 2016) have turned to Key Performance Indicators (KPIs) and Balanced Scorecards (BSCs) to assess their regulators. The BSC is a strategic management tool that tracks and manages performance across four dimensions: financial, customer, internal processes, and learning and growth. For regulatory authorities, this framework can be used to measure factors such as budget utilization, cost savings, customer satisfaction, stakeholder engagement, regulatory decision-making, industry compliance, employee training, innovation, and technology adoption.

3.3.5 GDPR regulator performance assessment

There is no standard performance assessment framework for the GDPR DPAs. The European Commission published a report in 2019 on the application of GDPR. The next one is due in 2024. The EDPB has published two reports (EDPB, 2021, 2022) that do contain some KPIs for some DPAs. Due to historic definitional and administrative differences, the KPIs are not entirely comparable and the second report does not include all the EU GDPR regulators. The DPAs publish their own annual reports, they are formatted differently and they can vary significantly in length. For example, the Irish DPA 2021 annual report (The Irish Data Protection Commission, 2022) is 119 pages compared to the 2022 report, which is 46 pages (DPC, 2023).

The European Ombudsman (EO) is an independent and impartial body that holds EU institutions accountable for their actions. The Ombudsman investigates complaints about maladministration by EU institutions and bodies. In 2021, a complaint (J. Ryan, 2021) was made to the EO that the EC was not collecting enough information to monitor the enforcement of the GDPR, particularly in Ireland. The outcome was an agreement that the EC would require a bi-monthly report from the Irish DPA (EO, 2022), which the EDPB expanded into a requirement for all member state DPAs to report on large-scale cross-border investigations (Lomas, 2023).

3.3.6 Motivation Summary

The GDPR regulator's mission is to safeguard data protection rights, which involves upholding individuals' information rights and data privacy. What does that mean in practice, and how do we know if they are doing a good job? Governments and the EU have struggled to answer this question, and there is a gap in the existing literature. This lacuna is important because regulators are key to achieving policy objectives. If regulators are to be made accountable and to learn best practices, an assessment framework, however imperfect, is required to score their effectiveness individually and relative to their peers. This has not been attempted before in the security community.

In Chapter 6, we will address how practitioners perceive regulators' effectiveness now and explore if there are better ways to measure it and thereby improve accountability and comparability going forward.

3.4 The Future of the GDPR

Having investigated the GDPR's impact on the three main categories of stakeholders, it is only natural to ask what might follow: how might the GDPR evolve over the next decade, and how might it affect said stakeholders? To answer this, I review sources drawn from academia, the professional advisory industry, politicians and the regulatory bodies themselves. Unsurprisingly, there is no consensus answer to this speculative question, which motivates the subsequent research methodology.

Academic literature addresses this question from broad, narrow and philosophical angles, but none are satisfactory. First, there are sweeping reviews such as "GDPR: Five Years After and the Future of Data Privacy Protection in Review" (Wodi, 2023), which concludes inconclusively "May we continue to live in interesting times". En route, the author predicts more collaborations with countries and companies in the area of adequacy decisions, the use of binding corporate rules (BCRs) and standard contractual clauses (SCCs) for international transfers, more data privacy impact and risk assessments, greater adoption of PbD and PET, and more emphasis on data localisation. In "Digital Empires: The Global Battle to Regulate Technology" (2023), Anu Bradford predicts that the GDPR will continue to shape global digital norms but face regulatory battles with the US. Big-picture reviews are valuable but too abstract for this study.

Second, pin-point reviews discuss the future complexity of international data flow and data governance across borders (Arner et al., 2022), future enforcement

outside the EU and strengthening enforcement within (De Hert, 2021), and the challenges of emerging technologies such as AI and data portability (Kuner et al., 2021). Third, there are reflective reviews such as "Complete and Effective Data Protection" (Lynskey, 2023) that argues that the attempt to make the protection offered by the law more 'complete' risks making it the "law of everything" and thereby jeopardise its practical effectiveness. However, none of these papers attempt synthesising these insights into holistic predictions.

In contrast, the professional advisory industry is not shy about speculating about the future of the GDPR, although it tends to be a word salad of generalisations (Donn, 2023), challenges (Spichtinger, 2024), or desirable changes (DPP, 2024). Sometimes, the insights are not all that insightful. For example *"the GDPR will have to adapt to evolving technology such as AI, Blockchain and IoT, the importance of global cooperation and Global Cross-Border Privacy Rules, and the need to balance innovation with privacy"* are insights hardly underappreciated (Sagacity, 2024).

In the UK context, there is concern about the pending new UK Data Protection and Digital Information Bill that will amend the UK GDPR and its impact on the UK's adequacy status with the EU. The fact that the EU has only concluded two other adequacy decisions since it came into effect in 2018 (Japan and South Korea) is seen as a systemic flaw with the GDPR (Dettling, 2024). So, too, is the situation where the EU and US are on their third data-sharing agreement, and it is once again being challenged in court. This is regarded as proof that the adequacy process sets unachievable equivalence standards. The current solution, which adds a "bridge of additional safeguards", is viewed as a bandaid, covering but not resolving the underlying legal differences between the two jurisdictions (Dettling, 2024). On the other hand, Hernández believes the principles-based approach of the GDPR gives it more than enough flexibility and caution against reviewing the GDPR with the inherent risk of opening such comprehensive and complex legislation (2024). They suggest those who demand reviewing the GDPR may be more interested in weakening it. These are interesting points but they do not paint a picture of where the GDPR will be in ten years.

Politicians are not known for being the shy and retiring type. Alexel Voss, a member of the European Parliament and one of the main drivers of the current GDPR, brings considerable expertise to the subject. In "Fixing the GDPR: Towards Version 2.0" (2021), he launched a public consultation and published a valuable critique based on the feedback. While his list concentrates solely on conceptual flaws, legal gaps and practical problems that occurred since the GDPR became effective in 2018, his document does not argue that the law itself should be withdrawn or its adoption was per se a mistake. Rather he believes the GDPR, in its current form, leads to compliance costs explosion and severely hampers Europe's digital transformation. Over 31 pages, he outlines fixes through legal adjustments as well as better guidance. Digital rights advocates, like NOYB, also regularly publish critiques of the implementation of the GDPR, and it is safe to assume they fed into Mr Voss's consultation.

Regulators, on the other hand, are renowned for their discretion for good reason. A careless or incautious forward-looking statement about a regulation may inadvertently move financial markets. Some academics (Hood, 2007; Stanley, 2019) believe there is a strong "negativity" bias at play whereby the principles of transparency and accountability are negated by a culture of blame avoidance.

It encourages regulators to develop policies and bureaucratic routines that minimise the risk of institutional or individual liability and blame. *"There is a paralysing fear of doing something that might be criticised"* (D. Davies, 2019). The national DPAs that enforce the GDPR are no different. Some are more outspoken than others but rarely speculate about changes to the GDPR. In May 2024, European Commission is expected to issue its Second Report on evaluating the General Data Protection Regulation (GDPR). This is a mandate of the GDPR itself that requires, in particular, to take into account "developments in information technology" (Article 97 GDPR). This report should provide an idea of changes if any in the future direction of the GDPR.

In the meantime, however, as outlined above, there is no consensus. None of the sources commenting on the GDPR has attempted to paint a future picture of it. For this reason, we employed techniques from the futures toolkit (GOV.UK, 2017), such as scenario planning, to answer the question, "How might the GDPR evolve?" which is presented in Chapter 7.

3.5 Literature review summary

This literature review provides an overview of the current research on the GDPR, focusing on three key stakeholders——business, the informed citizen, and the regulator—and its future potential evolution.

A significant body of research emerged pre-2018 in anticipation of the GDPR. The availability of draft text from 2014 and a two-year lead time after ratification in 2016 provided ample opportunity for businesses to adapt. This period witnessed extensive academic exploration of the GDPR's implications. However, there appears to be a paucity of research investigating the actual post-implementation impact, particularly regarding potential benefits for businesses. Chapter 4 aims to address this gap by examining whether the GDPR has yielded any positive outcomes for companies and how these benefits, if present, are distributed within the organization.

While research exists on public awareness of the GDPR, its focus often aligns with the commissioning body's agenda, leading to potential bias or superficiality. A significant period has elapsed since implementation, allowing for an assessment of genuine comprehension. This testing should encompass knowledge of the regulatory body responsible for enforcement, observed workplace changes, and the perceived impact of those changes on employers. However, a literature review reveals a scarcity of research employing such an approach. Hence, it was decided to address this gap with a comprehensive survey. Inspired by the famous L'Oreal advertising slogan "Because you're worth it", the research in Chaper 5 employs a reworked version and asks, "GDPR: Is it Worth It?" This reframing allows for a more nuanced exploration of public perception of the effectiveness and value of the GDPR.

A substantial body of work exists regarding the contested concepts of privacy, effective regulation, and regulator performance. However, there is a dearth of research specifically addressing the 'triple-contested notion' of data protection regulator performance. Chaper 6 aims to fill this gap in the literature. Ultimately, the success of a regulation depends on its execution. This research investigates the public's instinctive understanding of a data protection regulator's objectives and how they perceive them to be achieved. Furthermore, given

the absence of standardized data protection regulator performance metrics, the study explores the development of a more systematic evaluation framework.

Finally, while extensive discourse exists regarding the GDPR's challenges, limitations, and potential improvements, research that attempts to synthesize these discussions into a cohesive forecast of its future trajectory is lacking. Chapter 7 addresses this gap by employing scenario planning and future-thinking methodologies.

Chapter 4

"It may be a pain in the backside but..." Insights into the resilience of business after GDPR

4.1 Introduction

Regulation has long suffered an image problem for being boring, bureaucratic and unnecessary. While this can be true, we have shown in Chapter 2 that regulation remains a vital lever of government to achieve policy objectives. Governments regulate business to deliver better outcomes for the economy, the environment and society: for example to correct market failures, to protect people and wildlife from pollution and to safeguard citizens' privacy. The EU's GDPR is a good example of the latter and is a major disruptor in the context of data privacy and security.

Our focus is on an overlooked stakeholder: business. Most attention has concentrated on the benefits of GDPR to the regulator in terms of stronger powers and to the consumer in terms of stronger privacy rights. However, as we have shown in Chapter 3, little research has tracked the benefits to business who, after all, have had to substantially modify their sociotechnical systems to operate it.

While regulation is viewed by most as all stick and no carrot, the EU promoted and continues to promote the benefits of the GDPR to business. For this reason, we conduct exploratory research to understand the impacts on and resilience of business in the face of this major new disruptive regulation. In particular, we investigate if GDPR is all pain and no gain. Using semi-structured interviews, we survey 14 senior-level executives responsible for business, finance, marketing, compliance and technology drawn from six companies in the UK and Ireland.

RQ1: What are the perceived benefits of GDPR to business?
RQ2: Where are the effects of GDPR felt within a business?

We describe our methodology in Section 4.2, analyse the findings in Section 4.3 and discuss the findings in Section 4.4. We find the threat of fines has focused the corporate mind and made business more privacy aware. Organisationally, it has created new power bases within companies to advocate GDPR. It has forced companies to modernise their platforms and indirectly benefited them with better risk management processes, information security infrastructure and up to date customer databases. Compliance, for some, is used as a reputational signal of trustworthiness.

Many implementation challenges remain. New business development and intra-company communication is more constrained. Regulation has increased costs and internal bureaucracy. Grey areas remain due to a lack of case law. Disgruntled customers and ex-employees weaponise Subject Access Requests (SAR) as a tool of retaliation. All small and medium-sized businesses in our sample see GDPR as overkill and overwhelming.

We conclude in Section 4.5 that the GDPR may be regarded as a pain by business, but it has made it more careful with data. It created a short-term disruption that monopolised IT budgets in the run-up to GDPR and created a long-term disruption to company politics as Compliance and Information Security leverage the regulation for budget and control. The rising trend in the number of fines issued by national data protection regulators and the establishment of new case law will continue to reshape organisations. We believe this is the first study to analyse the lived experience of GDPR by business and the first to identify how GDPR has changed the balance of power and decision-making within organisations.

4.2 Methodology

Due to the newness of the issue and the absence of reliable data, we decided to take an exploratory qualitative research approach and use thematic analysis on semi-structured interviews.

4.2.1 Data collection and analysis

Data was collected via a series of semi-structured one-to-one interviews with business executives who work in companies that handle customer data. The study covered a range of small, medium, and large companies to maximise the sample's representativeness. It deliberately targeted senior and middle-management executives drawn from across the various functions within an organisation to get as holistic a perspective as possible. It included two Chief Executive Officers (CEO), three Managing Directors (MD), one Chief Marketing Officer (CMO), one Chief Information Officer (CIO), one Chief Information Security Officer (CISO), one Finance Director (FD), three senior legal departmental heads and two marketing executives drawn from public relations (PR) and digital marketing analytics.

The interviews were conducted over Microsoft Teams in April and May 2021 during one of the Covid lockdowns across Europe. Ironically, this situation probably made it easier to access senior executives and made the conversations more relaxed as they were speaking from home rather than if the interview had been arranged in an office context pre-Covid. The interviews lasted, on average

an hour and ranged between 35 and 90 minutes. The interviewees (9 male, 5 female) were aged between their early 30's and early 50's.

The interviews had a mix of open and closed questions. The open questions preceded the closed questions. The agenda for the open questions was very straightforward, namely asking executives what were the advantages and disadvantages of GDPR, based on their experience of it, within their companies. The agenda for the closed questions was developed by drawing on the literature review and capturing the predicted benefits and challenges. These were used as a checklist to ensure all the talking points were covered if they did not come up unprompted in response to the initial open questions. The interviewer's aide memoire can be found in Appendix A.

After conducting the first few interviews, we decided to add extra open questions at the end because we found participants had warmed to the subject by then and naturally opened up about how they would improve GDPR or how life would be different if GDPR had never happened.

One author conducted all the interviews to maintain consistency. The interviews were recorded and a report was written immediately after each meeting to summarise the main points. The research team reflected on the findings after each interview to identify common themes and resolve differences in interpretation. This initially caused the interview framework to be revised marginally.

The interviews were transcribed using automated transcription software and manually edited for correctness. This was followed by inductive thematic coding by the primary researcher based on the transcripts. This approach for analysing qualitative evaluation data (Thomas, 2006) condenses raw data text into brief themes, which can be used to develop a model or theory about the underlying structure of experiences evident in the data. The codes in this research were initially generated from the literature review and expanded as the interviews unfolded. Each code was manually transformed into a post-it note and clustered on a whiteboard to generate themes. This manual approach allowed us to easily iterate the analysis, and it facilitated cross-checking with the other researchers. We experienced a dramatic reduction in new themes after only a few interviews, in line with previous research (Guest et al., 2020). We felt that saturation had been achieved after 14 interviews.

4.2.2 Sample characteristics

It is difficult to recruit business people to dedicate time to an interview at the best of times. It is doubly difficult if the target is senior management and if the topic is a commercially sensitive matter. The interviewees were selected using convenience sampling. By networking through friends of friends and warm referrals, 14 senior executives agreed to be interviewed across six companies based in the UK and Ireland (which is in the EU). No attempt was made to reflect a representative group of practitioners based on EU geographic coverage. There was a conscious attempt, however, to diversify the sample away from solely IT or GDPR practitioners. The company classification is based on the number of employees (OECD, 2022) and shown in Table 4.1.

P1 was the owner-manager and sole employee of a technology solutions integrator with a turnover <£750K. It operated in the UK only. P2 to P5 were the senior management team of a small publisher with circa 30 staff that published specialist magazines for the UK and overseas markets. P5 and P6 worked at

the HQ of a light engineering manufacturer with circa 100 staff. It exported to mainland Europe. P7 and P8 belonged to a global drinks company and were based in the Irish subsidiary. P9 and P10 worked at the UK HQ of an international legal practice with offices in Europe, Asia and the U.S. The country practices are all independent practices under a common brand. P11 to P14 worked at the London-based global HQ for a banking and asset management company. The CISO and CMO held global responsibility.

Table 4.1: The organisations and interviewees labelled P1–P14

Size	**Sector**	**Job Title**	Labels
Micro	Technology	MD	P1
Small	Publishing	CEO	P2
		MD	P3
		FD	P4
Medium	Manufacture	CEO	P5
		IT MD	P6
Large	Drinks	Legal	P7
		Marketing	P8
Large	Law	Legal	P9
		CIO	P10
Large	Bank	Legal	P11
		CISO	P12
		CMO	P13
		PR	P14

4.2.3 Ethical considerations

The authors' departmental Research Ethics Committee approved this study. It is designed to include pseudonymity, confidentiality and informed consent. The study does not identify individual participants. All identifiable information was stripped from the transcripts and the recordings were subsequently deleted. Some quotes were altered or redacted to mask details. The participants were aware of the research's purpose, the researchers involved, and their role in it. Participants were not offered any compensation for participating.

4.3 Findings & analysis

This study investigates if there are any beneficial impacts to business from GDPR and how they are distributed across the organisation.

In this section, an expansive definition of 'benefit' is taken because benefits in business come in many guises. Typically, companies will classify benefits as

either direct or indirect. Direct benefits have a clear cause and effect relationship, whilst indirect benefits are less clear cut. A direct benefit will generate new revenue or reduce costs and is quantifiable. An indirect benefit, sometimes called a soft benefit, may be less tangible and defy direct measurement. Benefits may be planned or unanticipated. Benefits can also be in the eye of the beholder: what advantages one part of an organisation can disadvantage another. And finally, as discussed earlier in the section on regulation, what benefits a company may or may not benefit the consumer and society.

Our framework for discussion is based on themes that were generated by analysing and abstracting the interviews. The small sample size should be considered when judging the findings' generalisability. We will show that many of the impacts attributable to GDPR are a win-win for both business and the consumer/society.

Four positive direct impacts and two indirect impacts are identified; and while the primary focus of the research was benefits, we identify five challenges with implementing GDPR.

The participants were invited to suggest how GDPR could be made better. We review their feedback in the final section.

4.3.1 Direct impacts

4.3.1.1 Privacy-aware mindset

All interviewees stressed the importance of protecting data and privacy. On closer questioning, the motivation became clear. It is driven by fear. GDPR fines focus the mind. For severe violations listed in Art. (5) GDPR, the fine framework can be up to €20 million or up to 4% of global turnover, whichever is the higher. A compliance officer put it succinctly: *"Data breaches [...] gives everyone an incentive to listen [...] the 4% [...] is hanging over the heads of the board"* (P11).

The threat is felt by small and large players alike. The FD of an SME put the effect of a fine in a stark manner, *"we're running on fumes most of the time anyway, so any little thing could push us over the edge financially"* (P4). The CMO in one of the larger companies said,

> *"Data breaches and liability fines [...] We do simulated exercises around crises [...] and they always come down to a cyber hack and data leakage, and data is what we run our business by. So generically, it is the thing that keeps me awake at night the most, and it is the one thing that could blow our company up."* (P13)

GDPR has made executives more aware of data privacy both at a corporate and at a very personal level.

> *"We were very aware of its arrival [...] it approached us as something of a tidal wave of regulation because we knew that the sanctions against companies that failed to adhere were going to be quite stiff. And we also understood that it was important. We all have personal lives and know what it's like when we have interference and intervention and unnecessary and unsolicited approaches by organisations."* (P3)

GDPR has changed companies' data use behaviour. A marketer put GDPR's impact on spam as follows:

> *"As painful as it might be, fundamentally what it allows us to do is to understand our customers desired level of engagement with our company. [...][In the] wild west before GDPR came along [...] you didn't have to bother about things like marketing permissions and things like that.[...] [You used to] have a mass of customers; you used to contact them through whatever means whenever you wanted to, and some were more receptive to that than others."* (P13)

GDPR has changed corporate attitudes. As one executive observed *"It does put the whole of the organisation into a different mindset"* (P12). It has raised *"awareness within the business around personal data, the importance of protecting it and treating it in specific ways"*. (P7) It *"has led to a better understanding of why we hold data"* (P7). It stops people from hoarding data and gets rid of the *"just in case mentality"* (P9).

It has also *"raised awareness within the business from a cyber perspective [...] which has resulted in us procuring cyber insurance"* (P9). *"Security is tighter now [...] in terms of encryption [...] we've tightened down access"* (P7).

In sum, the threat of GDPR fines has made companies become more responsible. As one CEO put it, *"I suppose we just are a little bit more careful what we use the information for"* (P2). That is clearly a benefit to consumers and society and arguably helped business become a better corporate citizen.

4.3.1.2 Spur to change

New regulation like GDPR may require companies to change their people, processes or technology. It depends on how close their model of operation was already in alignment with the new regulation. Suppose a company is forced to buy a new data system to satisfy GDPR and the new system delivers new efficiencies and cost-savings. In that case, it is difficult to argue that they are direct business benefits of GDPR. After all, the company could have used that same money for something more value generative such as new product development or expansion into new markets. However, if a company is forced to face up to longstanding issues that it knew had to be fixed or it would decline, and if GDPR is the spur to make that investment finally happen, then it is arguable that the spin-off benefits can be regarded as a direct benefit to business from GDPR.

Out of the six companies in the study, two made minimal changes to their IT infrastructure. One tweaked their data classification *"It was just about reconfiguring it"* (P10). One was created after 2018 and was designed from the outset with GDPR in mind, and the remaining two were spurred to make fundamental changes. In both cases, GDPR *"got us to shift change at a quicker rate than usual"* (P7).

One of the SMEs said the most significant benefit of GDPR was *"getting things in order"* (P4). *"We had enough spreadsheets to fit in a football field"* (P4). They moved everything onto the cloud, went paperless, slashed costs and reduced headcount by 2/3rd. In effect, GDPR meant *"driving the digitalisation and automation of a lot of systems [...] and the restructure of the organisation"* (P6).

In contrast, one of the larger companies had already concluded that data-driven marketing *"is the way of the future"* (P8). It used GDPR as an opportunity to centralise all country customer databases in global headquarters (GHQ), standardise the data input and output processes, tighten access control and upgrade information security. It required all customers to re-opt in as part of a campaign to be GDPR-ready. It programmed standards into the workflow to enforce GDPR principles such as data minimisation and data retention periods and made it apply worldwide. As an example, the company now has an automated rule that flags and deletes prospect data if they have not been *"touched"* (P8) after a year. It also serves as a feedback loop between country management and GHQ. Why have you neglected to contact these prospects? Did a mass campaign target the wrong market?

Did GDPR spur innovation? All six companies initially said no when asked directly and then gave examples that sounded curiously like a new service or marketplace. The technology SME had added a self-service facility so that clients could interrogate and edit their own details, i.e. a do-it-yourself SAR. The IT outsourcer's business had boomed as it raced to develop new services to respond to clients' GDPR-related demands. Likewise, the law firm had had to recruit extra staff to handle the GDPR workstreams, opened a new branch office in the US to advise local firms with interests in Europe and expanded a GDPR-compliant legal technology platform service to its clients who needed to pool and overview legal matters internationally. The bank noted it had seen the RegTech sector expand which meant it had a wider selection of GDPR compliance systems to choose from.

To sum up, GDPR made companies upgrade their IT, some superficially and some more fundamentally and, it has spurred growth of the GDPR support services industry.

4.3.1.3 Reputational signal

Reputation management is about sending the right signal to the right stakeholder. Does GDPR compliance by a company, communicated via their public privacy policies and online cookie consent notices, enhance a company's brand and reputation? Do consumers trust it more? Interviewees tied themselves in knots considering this. Many started with a flat *"No"* or, slightly less dismissively, *"I don't think it is high up in people's minds [...] since the legislation is no longer a choice and we all have to be compliant"* (P2) or *"it's a minimum standard"* (P3). The recognition *"it's a necessary element of doing business"* (P1) morphed into *"I think failure to do it can impact negatively"* (P7) and *"It is a hygiene factor. If you are not GDPR compliant, you've got a problem"* (P10).

The concept of hygiene factors dates to psychologist Frederick Herzberg's two-factor theory of worker motivation (Herzberg et al., 2017), which marketers later adopted to mean the basic set of values that customers expect to be in place for any business or service they consider purchasing. In mathematics, it would be described as a necessary but not sufficient condition. *"Everyone wants to see that you are obeying looking after your data"* (P4). When asked about trust, a lawyer said, *"The customer expectation is higher. I'd say expectation more so than trust is higher"* (P7). In contrast, a marketer said, *"People are looking for brand purpose. They're looking for brands with meaning. They're looking for a brand with authenticity. They're looking for brands that do the*

right thing" (P8). Referring to marketing communication, another said, *"From a client point of view, they know that you are only sending them stuff that they want to receive"* (P14).

So, some companies regard GDPR merely as a box to be ticked and some regards it as a signal and trust builder. Some use it to send a signal of *"reassurance"* (P14) that the consumer will not be spammed. Some use it to say we care about your data, and you can trust us. In fact, one CISO believed that their ISO27001B certification was an indirect benefit to the customer because it tells the customer *"we actually take security seriously"* (P12). In an online world where service experience is relatively undifferentiated, reputation is a key differentiator and GDPR compliance may now be part of it. Half of the sample chose to regard it as a lever and half thought it was a hygiene factor at best.

4.3.1.4 Standardisation

Standardisation is often seen as a positive output from regulation. The theory is that technical standards facilitate faster economies of scale on the supply side and provide the comfort of mind to encourage more rapid take-up on the demand side. GDPR might seem an unlikely exemplar, but three cases came to light that delivered direct business benefits.

In the first case, a small and medium-sized enterprise (SME) that did a lot of business with the public sector described how time-consuming it used to be to bid for a new project because each *"organisation would write their own requirements around privacy"* (P1). Now GDPR has made responding to formal tenders for new business a quick box-ticking exercise instead.

In the second case, the drinks company standardised its customer database *"so for an international company we have a lot more consistency and assurance across the group"* (P7). It used to have to consult individual countries on the online and offline product packaging before every new product launch. Now GDPR means they can save time and say *"here is a policy and here is a language"* (P7).

In the third case, the banker liked the way GDPR neutralised a perceived weakness relative to more aggressive banks *"From a marketing perspective, the fact is that we all had different interpretations of what you can and can't do"* and approval sat with *"how strong our risk function was and [...] how militant it was. That is where oversight was"*. He felt *" you are at a competitive disadvantage with a stronger risk function."*(P12) but now *"it's good to know that all companies are legally bound by these GDPR rules"*.

The last example may also qualify as a demonstration of the benefit of a level playing field which the EU regularly messages as a benefit of EU-wide regulation in general. Not all respondents accepted this rationale behind GDPR and felt that the EU was *"trying to make it sound more for the companies but we all know it was for the consumer. They did it for people rather than the companies"* (P11).

4.3.2 Indirect impacts

4.3.2.1 Powerful GDPR advocates

Andrew Jackson, seventh president of the United States, is credited with the saying *"money is power"*. Within companies, this translates into budget is

power, and nowhere is this more apparent than the power that GDPR has conferred on specific roles within companies to invest in compliance. One lawyer was quite frank:

> *"I am a boring lawyer, but I think the fact there's robust legal obligations has made business ensure compliance at a speedier rate than usual. [...] The level of fines makes for a great headline when you're running training and trying to get everyone's appreciation."*
>
> (P7)

GDPR has transformed the authority of the department responsible for it—usually Legal, Risk or Compliance—and made it an essential player in corporate data-related decision making: *"It has raised awareness of the compliance team. [...] People take compliance a lot more seriously"* (P9).

It may seem the main benefit of a beefed-up GDPR-legal resource is fine limitation. The lawyers cited other benefits such as reduced paper storage costs, greater awareness of the importance of cyber insurance, tighter scrutiny of third-party supplier contracts and more attention to where the data in the cloud resides to ensure the EU GDPR regime covers it.

4.3.2.2 Improved data management and security

The other budgetary beneficiary is the IT department. One CISO (P12) believed GDPR *"did raise the bar for visibility of information security [...] in the past [...] it was regarded as a nice to have. [...] Not many companies actually had a security department"*. This CISO also thought that *"GDPR focused people's minds that if you let the data get out, then it could conceivably bring down the company"*. Another CISO (P10) described how they work with risk and compliance to document risk and list controls they had against those risks so that when they suffer a breach, an inevitability in their view, they can demonstrate to the regulator they had made a proportionate investment to meet their obligations to the spirit and letter of the legislation.

Thus, the budget has been invested in information security infrastructure, resilience, and eliminating single points of failure. Another focus is security awareness training for the workforce. The investment has resulted in streamlined processes, efficiencies and cost savings. It has motivated companies to take a holistic view of security rather than *"sticking the firewall in the way"* (P12). It has meant that the customer database is constantly cleansed and deduplicated to ensure client notification preferences are up to date, which in turn means the advertising is targeted at customer and prospective customers who are genuinely interested in the company's product or service. As one marketer put it, prior to cleaning up our data and duplicates, *"we used to have multiple versions of the truth"* (P13).

4.3.3 Challenges

4.3.3.1 New business development is harder

A key part of new business development is identifying, qualifying and converting suspects into prospects and prospects into customers. A pipeline of leads is

generated via a variety of means such as advertising, social media and email marketing campaigns.

The biggest drawback of GDPR for one SME was *"finding effective ways to find new customers"* (P1). He recounted how, before GDPR, their resellers made it a precondition that users had to agree to receive spam before their service was activated. Even though it has been against EU law to send unsolicited commercial emails or texts for almost 20 years, it seems to have taken the introduction of GDPR to get the message finally through to business because it changed the rules of consent and strengthened people's privacy rights.

Smaller companies felt GDPR had little effect on them since they were never great spenders on advertising in the first place. However, on exploring the application of the data minimisation principle, there was a dawning realisation by all the SMEs that it had affected them. In practice, they had stopped asking for more information than strictly required so that it could be used again in later campaigns. Previously, they used to periodically re-market to historic enquirers, ex-customers, or lapsed subscribers as a matter of routine.

Larger companies thought it had made their marketing more targeted and effective because they only communicated with genuinely engaged consumers who had already opted-in to receive marketing communications: *"GDPR forces us to categorise customers according to their wishes and to segment the communication we send them"* (P13).

The flip side for marketers is that it made it harder to build the brand if they were only allowed to talk to the *"converted"* (P8). It also made it harder for IT in large companies if they had multiple streams of leads (referrals from the parent company or associate companies, web enquires, responses to marketing campaigns, Facebook, Linkedin, Twitter, Google ads) because they had to deduplicate the customer to ensure their preferences were captured correctly and thereby avoid complaints about receiving unwanted marketing communications.

4.3.3.2 Direct & indirect costs

How companies experience the cost of regulation varies widely. One SME remarked he expected the costs to be more, but their only cost was the *"minimal"* ICO (UK Regulator) fee (P1). Another SME believed their costs had gone up because they had moved everything to GDPR-compliant cloud providers and assumed their transaction fees included a GDPR component. In general, apart from explicit GDPR-related costs such as cookie notice plug-ins, SMEs found it difficult to pinpoint additional costs.

Larger companies found it easier because they had made more extensive investments in systems, processes and manpower. One company estimated *"15% of our legal budget in the last year was probably on data protection"* (P7). Another put it at less than 5% (P10). In addition to direct costs, there were indirect opportunity costs. A Global IT Director described GDPR as *"stifling"* and *"distracting"* (P10). He complained that GDPR projects always trumped other innovative projects such as process automation. Another complained that they had lost business due to GDPR because it made the company so reluctant to share referrals or client information with associate companies in other EU countries.

Attitudes to the added expense vary depending on the department. Marketing sees it *"as an additional burden"* (P11). They complain *"they have no time*

and no budget for it" (P11) and it makes their campaigns uncompetitive against players willing to sail closer to the wind. In contrast, IT see the bureaucracy as *"a cost worth bearing"* (P12) if it brings *"sensibility"* (P12) to an organisation.

4.3.3.3 Grey areas of law

Unsurprisingly, non-legal and legal interviewees had different perspectives on the state of the law. Most SME management did not have an opinion apart from a shared consciousness that they lacked in-house compliance knowledge. Some expressed worries about loose data hygiene by staff working from home. Some worried about SARs and how much disclosure was required. All thought they had outsourced responsibility for security under GDPR compliance to their GDPR outsourcers.

Participants who did have contact with GDPR complained simultaneously that GDPR was over-prescriptive and under-prescriptive. For example, some believed they should be trusted to use their professional judgement and take a risk-based approach to issues. Otherwise, *"GDPR is often like using a sledge-hammer to crack nuts over things [. . .] put barriers where they otherwise wouldn't need to be"* (P9). Others wanted more precision about technical solutions and data retention periods. Despite their best efforts to be GDPR compliant, one marketer bemoaned, *"how transparent is transparent? [. . .] how much do you really have to spell it out [. . .] to be really clear enough"* (P8) after the Legal department had blocked their re-use of data collected during a campaign that had been designed to gather new leads.

A lawyer described the ambiguity that they experience whenever they suffer a data breach: *"I regularly go to external counsel to get their view and they never have a definitive answer. It is always from experience, or we'll have to wait and see"* (P7). Another lawyer described how they pore over ICO investigations to understand the decision-making and the findings that triggered the fines.

Some worried about GDPR in the UK after Brexit if there is a negative EU adequacy decision. One IT executive in a large company described it as *"utterly bonkers"* (P10) because *"the damage it would do to both the UK and European economy would be just politically unacceptable."* The executive also thought they'd have to have two platforms—UK and non-UK—if the EU failed to find the UK was offering an adequate level of data protection.

4.3.3.4 The data audit dividing line

Data audits distinguish the big from the small. When asked about the impact of data audits on their business, one SME responded, *"What's a data audit"* (P1). Two other SMEs were uncertain and assumed their GDPR IT outsourcer had taken care of it. On follow-up, one of the IT Services companies confirmed they stored the data and advised their clients, but *"this is where it gets a little bit complicated [. . .] they need to know where the PII is themselves"* (P3).

Large companies approach it differently. They all do data audits. They find them time-consuming, but they appreciate they are *"a good thing"* (P7). One IT executive remarked, *"It may be a pain in the backside, but once you've done it once, then at least you know where everything is. [. . .] And you will be able to follow data around your organisation"* (P12). Another lawyer described how they had undergone two audits—-in-house and external-—and opined: *"I found*

the audits helpful [...] you can leverage off [...] and show the reports to the directors and say either look how well I am doing in this area [...] or we scored low here" (P7). Data audits are powerful tools in big business for building business cases for investment.

4.3.3.5 The weaponisation of Subject Access Requests (SARs)

One SME has never received a SAR. In another SME, the CEO had dealt with a handful personally. As companies scale up in size and customer base, satisfying SARs can become more challenging.

The CEO of a medium-sized company described vividly the pain of dealing with disgruntled customers who use SARs

> *"as a stick to beat us with. They'll put in a SAR [...] just to be awkward. They're saying '[...] you have inconvenienced me, so now I'm going to inconvenience you.' Are they entitled to every internal email? They have rights to everything, but I'm saying, 'but why? Why should they?' [Perhaps] we'll do it offline [in future]."*
>
> (P2)

Larger companies described similar issues with customers and, even more problematic, ex-employees. Some companies found it difficult to differentiate between emails that plainly referred to the ex-employee and deserved to be released and those that mentioned the ex-employee in a performance report alongside other employees. *"We've had an employee one that was horrendous [...]going through emails at what you can redact [...] I've seen from an employer perspective and it's very much weaponized"* (P7). Other companies adopt a more proportionate response to SARs and require a precise aim.

Actioning the right to be erasure is also problematic *"the systems are not set up to make it easy to remove those people. It's not built into Microsoft systems. There is not a right to forget button that goes right across all your Microsoft systems files and folders"* (P12).

4.3.4 Suggested improvements to GDPR

At the end of the interviews, people were asked for their ideas on how could GDPR be made better. There was a certain amount of special pleading and wishful thinking. Nevertheless, the feedback points to ways in which GDPR could be made more accepted and more effective in achieving its goals.

4.3.4.1 An SME-lite version

All the SMEs felt GDPR was overkill for companies like them that hold truly little data compared to Big Data companies. One CEO queried why they should be held to the same standard as a medical institution that holds sensitive personal data. *"The rules I have to follow should not be the same ones as Goldman Sachs has to follow"* (P5). The desire for simplification is understandable. Unfortunately the rights-based nature of GDPR hardly lends itself to differential watering down of protections for customers of SMEs but not of big business. Nevertheless, in practice, the regulator could consider applying the same principles on SMEs in a more proportionate manner.

4.3.4.2 Reframe it

A marketer suggested the regulator should demystify and reframe the message. *"Less a pain in the arse type thing [...] bring to the fore the real benefits [...] in a more creative way"* (P8). This may seem an unusual demand, but marketing spin is not alien to the EU Regulators. After all, most GDPR updates since 2019 usually include references to the benefits of the level playing field (LPF) and the competitive advantage to business of compliance. However, these messages do not resonate with this sample of companies. The LPF is irrelevant to SMEs who are typically domestic in focus and not material for larger companies if they already have operations in other countries. NOne of the respondents believed GDPR conferred a competitive advantage to them within the EU (because everyone must abide by it) and some saw it as potentially a disadvantage in non-EU countries if the competition is not saddled with the same restraints.

4.3.4.3 Share it

The GDPR expert in the bank felt the UK Regulator failed to support big business. *"There is nothing to encourage people or companies to share best practice. There is not a forum [...] or platform [...] where the professionals can go and ask questions or share what works for them"* (P11). At the other end of the expertise spectrum, the CEO of a SME felt let down for different reasons *"I looked for checklists [...] on government sites. Everyone is trying to get me to take a course to get a certificate in GDPR compliance"* (P5). All they wanted to know was *"what are the major things we should concentrate on"* (P5).

4.3.4.4 Clarify it

Most respondents thought GDPR had brought legal clarity to the situation. Article 6 of GDPR is clear about the six lawful bases for one to process (collect, store, use etc.) people's data. However, the legal practitioners still felt there was a need for clarity on the wording in some instances, e.g., co-processor, international data transfers. *"I did a Certificate in Data Protection Law [...] and at one stage I was about as qualified as you could be, which was a bit of a joke, because I didn't know more than anybody else. You go to talk to a law firm [about a case]. They have more experience but it's not necessarily they know more [...] until there is more case law"* (P7). Like the previous point about sharing learning, there seems a clear opportunity for the regulator to take a more proactive role in this area.

4.3.4.5 Loosen it

Some of the legal practitioners chafed against the rigidity of the rules. They argued that the regulator should allow a more commercial or risk-based approach of the rules for an informed professional such as happens with anti-money laundering. Questions remain about how this would work in practice including how such an approach is compatible with the fundamental rights character of data protection and how a risk-based approach could be made consistent. The other concern is the notion of risk itself and the risk thresholds (to the consumer?) that would need to be satisfied before GDPR could apply.

4.3.5 Counterfactual: What if GDPR didn't exist?

This counterfactual scenario was added to the agenda after it arose organically mid-way into the research. When asked what they would be doing differently with customer data if GDPR wasn't here today, the consensus was that they'd hold more data, hold it for longer, use it for multiple purposes and not worry so much about the security. *" I'd like to say it wouldn't be that different because we want to, [...] from an ethical perspective, [...] to put in these controls anyway, but I think that would be being a bit disingenuous. I'm sure that we just have a lot less control because we're not being forced to, so we just wouldn't. And. We would store data for a lot longer and we give a lot[...] more people access to the data"* (P10). The lost freedom to proactively market to ex-customers or cross-sell to other customers in different subsidiaries of the bank was uppermost in the mind of the CMO *"Ultimately the scale of our marketing opportunity would be that much larger"* (P13) if GDPR didn't apply today.

4.4 Discussion

4.4.1 The benefits of GDPR to business

Whilst one should be cautious generalizing from a small sample, our findings are drawn from broad-based conversations with senior and junior executives across the functional spectrum of organisations and they show that GDPR has had a common range of effects on business at large.

The threat of fines has changed the mindset of companies. In a world where data privacy is getting ever more important, GDPR has forced companies to catch up with their clients' desires and wishes to serve them only what they want to be served and use their data only in the way they want it to be used. It has forced companies to clean-up their act. This is a win-win for companies and society.

The threat of fines has changed the data infrastructure of companies. In a world where compliance projects trump non-compliance projects, GDPR has forced companies to modernise and upgrade their data management, data quality and information security. In possibly a one-off hit, GDPR has gifted companies a reason to invest in projects, such as rationalising legacy databases, that they knew were important but kept putting on the long finger. It has delivered many of the 'usual' benefits of an IT project directly to companies whose technology was sub-optimal and it has indirectly benefited companies whose technology was adequate but still required enhancements to meet the regulations.

Contrary to the common perception that regulation adds complexity, GDPR has delivered standardisation benefits by streamling processes in some situations cited in our research. It is also used by some companies to signal their privacy credentials in the belief it enhances their brand and reputation.

Our findings on benefits do not tally with many of the projected benefits in earlier literature. The area of agreement is around improved data management process (Bennett, 2018; Fimin, 2018), use of analytics (Garber, 2018) and increased security (Krikke et al., 2019). There is some equivocal overlap in the area of reputational enhancement (Beckett, 2017; Tikkinen-Piri et al., 2018). We found some marketing participants shared the same belief. However, many

of the other assertions such as improved consumer confidence (Dellie, 2019) and trust (Dellie, 2019; Dubrova, 2018), legal clarification (Dubrova, 2018), competitive advantage (Dellie, 2019) and cost reduction (Beckett, 2017; Miglicco, 2018; O'Brien, 2016; Perry, 2019) were not supported by our findings. The size of the GDPR fining system was well understood in advance, but the transformational effect it was going to have on corporate psychology was under appreciated.

4.4.2 The changing balance of power

Our findings show that the impacts of GDPR are felt differently within a business. It has created new power bases within companies. Depending on the industry, it will have a different name, but typically GDPR expertise sits in the Risk, Compliance or Legal department and the IT/IS or Information Security department. Both have enjoyed boosts to budgets and headcount. Suffering a high-profile data breach that could destroy a company's reputation and potentially suffering a big-ticket fine that could ruin a company's finances has meant that GDPR risk continues to be a board agenda item. This means both departments continue to be more involved with corporate-level data decision-making than before. It also means that Marketing has a high quality, more up-to-date database of customers and their communication preferences.

So, while Legal and IT may be winners, are there losers? Yes. There are direct and indirect losers. The most obvious are the executives spread across an organisation who championed projects that were delayed or killed in competition with higher priority GDPR initiatives. Less obvious are senior management. Their discretion was hemmed in pre-GDPR by the need to prioritise GDPR-readiness. Their discretion is now policed by Legal or IT departments who follow breach investigations zealously and remind them that GDPR compliance is an ongoing commitment. The indirect losers are the departments that have to handle the extra workload generated by GDPR compliance, e.g., Human Resources having to negotiate with disgruntled ex-employee SARs, Customer Service having to deal with dissatisfied customer SARs and Marketing having to constantly update customer notification preferences. A lawyer said *"I think if you were to ask a marketing person what are the benefits [...] I think they might struggle to articulate some benefits"* (P7). Another lawyer characterised the perception of their role and GDPR, *"From a marketing perspective [...] they see it as a stopper"* (P11).

A lasting legacy of GDPR is a shift of power. It has put non-commercial functions, which were hitherto regarded as support functions, at the heart of strategic decision-making. The long-term implications of this remain to be seen, but one can make some educated guesses. As GDPR beds down and regulators become more comfortable issuing fines (based on precedents in other EU countries), the influence of these groups will increase rather than decrease. Senior management will become exasperated with box-tickers and binary thinkers and may seek to recruit people with different skill sets and risk appetites. Conversely, if enforcement by regulators is timid and the threat landscape is perceived to be less draconian than expected, senior management may decide to game the system and put the box-tickers back in their box.

The introduction and operation of GDPR is not a rational application of a new data protection regulation. It is a benefit, a tool or a weapon of power whose promotion is contextualised by different groups within an organisation that have

different aims and methods of leverage. Even actors, such as ex-salespeople who would normally rail against GDPR constraints, weaponise SARs to their own ends creating unintended consequences.

To the best of our knowledge, this disruptive change in power dynamics has not been anticipated in earlier information security literature.

4.4.3 Implementation issues remain

GDPR is not without its disadvantages. This was not the primary focus of our research but we identify a number of challenges. New business development and intra-company communication is more constrained. Regulation has increased costs and internal bureaucracy. Grey areas remain due to a lack of case law. Disgruntled customers and employees weaponise SARs as a tool of retaliation.

Our findings on challenges tally with many of the issues identified in earlier literature. The complexity of GDPR, its lack of specificity, its subjectivity, the cost overhead, the difficulty recruiting and retaining expert staff and operationalising the right to erasure were all well anticipated. The restrictions on marketing were known in theory but the effect on new business development in practice was underappreciated. The chilling effect on intra-company communication does not appear in earlier literature. On the other hand, some hypothesised downsides, such as companies withdrawing services in the EU to avoid GDPR, did not ever come up in conversation.

When we asked our participants for ideas as to how to improve GDPR, we find that they believe that regulators should re-frame GDPR messaging to be more positive, sponsor forums to facilitate the sharing of learning and coping strategies, clarify policies and apply lighter standards on small business.

Existing literature does not consider getting business buy-in to GDPR. The emphasis is more on the punitive power of GDPR. In contrast, the literature has long recognised the need to simplify and clarify its requirements.

4.4.4 Limitations & future work

There was little empirical research to compare and contrast our findings. The study is based on a small sample size and may affect generalizability confidence. The participants do not have the same job profile in each company. This is partly due to smaller companies having general managers who hold multiple briefs and larger companies having executives who are responsible exclusively for a department such as technology or compliance.

A limitation endemic to interview-based research is response and social desirability bias. Respondents may have over-reported positive or negative effects to please the interviewer. Another common limitation is interviewer confirmation bias. In this case, the author began the project believing there were no positive benefits to business and was pleasantly surprised to discover there was a wealth of research findings of both a positive and negative nature. Finally, it is never clear how to weigh subjective benefits, although we partly addressed this via RQ2 by asking where the positive and negative effects of GDPR were felt within an organisation.

Future work could pursue several avenues. One could repeat the research with a larger sample population to support the generalisability of any findings; or repeat the research in other EU countries or industrial sectors and compare

the differences; or analyse and compare how the power dynamics evolve within companies as the real risk of fines becomes clearer over time; or analyse the enforcement records of national regulators and the perceived compliance of industry in their jurisdiction. Alternatively one could review recent initiatives to make GDPR more proportionate in its application to SMEs whilst maintaining consistent protection of consumers' rights.

4.5 Conclusion

GDPR is a regulation that is designed to safeguard EU citizens' data privacy. The benefits to the consumer and the regulator and the downsides to business are relatively predictable. What we were interested in exploring however is whether there are any benefits of GDPR to business and how they might affect the different parts of an organisation. To our knowledge, nobody has looked at this from the perspective of business since GDPR came into effect in May 2018.

Using semi-structured interviews, we surveyed 14 senior executives responsible for business, finance, marketing, law or IT drawn from 6 small, medium and large companies in the UK and Ireland. We deliberately sampled beyond the IT department, which tends to be the typical target of GDPR surveys, to obtain a fuller picture.

We find the threat of large fines has focussed the minds of business and made it more privacy conscious. GDPR has gifted companies a reason to justify investment in modernising their data management processes and security. Companies have cleaner and more up-to-date customer databases. In the absence of GDPR, companies admit they would ask for more information than necessary, use it more frequently, hold it for longer and keep it less securely.

It has created new power bases within organisations that act as guardians or champions of privacy. Such in-house regulators will continue to enjoy influence on corporate decision making provided the regulators maintain a steady news flow on enforcement actions against offenders and data breaches.

We find that many implementation issues exist that would benefit from better communication, guidance and simplification by the EU and its regulatory arm.

To sum up, GDPR may be a headache to business but it has made it more careful with data. Judged by that standard, GDPR has been a successful socio-technical regulation because it has made companies put their house in order to their own benefit and to the benefit of wider society.

In the next Chapter 5, we expand on these findings by focussing on individuals who have worked in the same company before, during and after the rollout of the GDPR. They will have observed and potentially implemented changes in their workplace as a result of the GDPR and will be aware of the costs and benefits to their employer and to the improvements in their consumer rights as ordinary members of society. Essentially, we ask this group of workers who are uniquely informed of the trade-offs: was the GDPR worth it?

Chapter 5

GDPR: Is it worth it? Perceptions of workers who have experienced its implementation

5.1 Introduction

People who were employed before May 2018 and who are still employed by the same organisation will have experienced the impact of the GDPR on their workplace first-hand. They both implement it as employees and benefit from it as consumers. The goal of this chapter is to understand the unique dual perspective of this group.

The GDPR has been studied from multiple points of view. It ranges from the implementation challenges business face (Poritskiy et al., 2019a) to the enforcement issues Data Protection Authorities (DPA) face (Chazal, 2024; Grant & Crowther, 2016; Johnson, 2022; J. Ryan & Toner, 2020) to the operational realities that consumers face (Nouwens et al., 2020). The European Commission (EC) and professional services firms have surveyed consumers' awareness of their rights and businesses' awareness of their obligations. In academia, there have been reactance studies (Strycharz et al., 2020) and comparative awareness studies across Europe (Rughinis et al., 2021). Unlike previous perception studies that focused solely on consumers or data professionals however, this is the first empirical research into how these informed individuals perceive the cost-benefit of their rights as consumers balanced against the pressures they see it places on their employer to support those rights. Using a multi-stage survey N=10 & 273 & 102, we explore a series of hypotheses to arrive at our research question—GDPR: Is it worth it?

To exercise their rights, consumers need to be aware, to some extent, of the regulator's identity, role, and powers. The EC (Belgian DPA, 2021; European Commission. Directorate General for Justice and Consumers. & Kantar., 2019; Great Britain & Information Commissioner's Office, 2021; PR Newswire, 2019) and some DPAs have conducted consumer awareness and confidence surveys but

we find little evidence of systematic overt publicity campaigns. We test if our informed citizens know who their regulator is and what they expect of them.

Most business-focused coverage of the GDPR in the media concentrates on data breaches and regulators' fines (Chazal, 2024; Venkataramakrishnan, 2021; Wolff & Atallah, 2020). It stresses the deterrence effects of the GDPR sanctions at the expense of any incentive to change or upside for business. If the point of privacy regulation is behaviour change (Coglianese, 2012; The Environment Agency, 2011), measuring it is difficult. Available data, such as the number of fines, delivers a highly imperfect and incomplete picture of compliance within companies. Instead, we test what GDPR-driven changes have been observed by our respondents within their organisation and if they believe these changes have been net-positive.

At the end of the survey, after making our respondents consider the GDPR from multiple angles, we ask if they feel the GDPR has been worth it. Their answer is important because it cuts to the heart of privacy in the digital age. Without data protection, citizens will arguably be exposed to more profiling, monitoring and mass influencing by digital advertisers and/or the state. We find the informed citizen-consumer does buy into the GDPR, with all its positives and negatives. They recognise their rights when prompted but know little about their regulator. They have observed concrete changes to data practices in their workplaces and appreciate the trade-offs. They take comfort that their personal data is handled as carefully as their employers' client data. The very people who comply with and execute the GDPR consider it to be positive for their company, positive for privacy and not a pointless, bureaucratic regulation. This is rare as it contradicts the conventional negative narrative about regulation. Policymakers may wish to build upon this public support while it lasts and consider early feedback from a similar dual professional-consumer group as the GDPR evolves.

Section 5.2 describes the survey design and data analysis, Section 5.3 presents the results and Section 5.4 & Section 5.5 draw out several high-level themes and their implications from a theoretical, managerial and regulator perspective.

5.2 Methods

The hypotheses underlying the research question lend themselves to qualitative and quantitative analysis. Interview and experimental methods were considered and discounted. Recruiting individuals at scale who have been in continuous employment for over five years from diverse organisations is, unfortunately infeasible. Thus, a survey-based method was both a sensible and a realistic option.

An early key decision was to limit the survey to the UK. The GDPR may be the same across the EU but the composition of the national regulators and how they implement the regulation are very different for historic reasons. Expanding it to mainland Europe may seem an attractive opportunity to consider a broader cross-cultural perspective but it also came at the cost of introducing too many variables into the study.

5.2.1 Design

The survey was developed in three phases: a test to check interest, a test to check potential population size, and the final study. Participants were recruited via Prolific, an on-demand platform for connecting researchers with volunteers worldwide. The data was collected using the Qualtrics survey platform between the 30th of May and the 16th of June 2022.

In phase #1, N=10, we used a fast one-minute survey to test the strength of interest in the topic, as we noted some research topics lay ignored for weeks on the platform. In phase #2, N=273, we used a longer three-minute survey to confirm there were enough individuals with relevant experiences on Prolific to warrant a full study. To ensure respondents had worked pre-and post-GDPR in the workplace, we pre-screened respondents to have at least 5 years of tenure with the same organisation. We also asked if they had heard of the initials GDPR. If they answered the initials were unfamiliar to them (only 7% of respondents), they were paid, thanked and dropped from the survey. It did provide a measure of unfamiliarity or basic unawareness of the GDPR. We found respondents answered the survey suspiciously quickly, so we redesigned the survey to add more nonsense and attention checks, repeated and reworded some questions to measure response consistency. The final survey design can be found in Appendix B.3.

Based on the responses of phase #2, we expect to find a medium-sized effect (≈ 0.5) in the main study. For one-tailed repeated measures t-tests at a significance criterion of $\alpha = 0.05$, the minimum sample size is 45 participants. To give room for Bonferroni corrections a sample of 90+ should allow us to achieve statistically significant and generalizable results.

Thus, in phase #3, we recruited N=102 participants. A representative demographic distribution of the UK was enforced in sampling from the phase #2 database to make the research findings more generalisable. The final sample shows an appropriate distribution in terms of gender, age and education compared to census data and consists of 51 female and 51 male respondents with an average age of 45 years for both sexes. Answering the final survey took 10 minutes on average. Seven participants failed exactly 1 of the 7 nonsense, attention and consistency checks. No one failed more than one, so we did not exclude any responses from our analysis. A statistical analysis of mouse and keyboard browser events showed that participants paused and answered questions thoughtfully. This proves we have high-quality responses.

5.2.2 Data analysis

The survey consisted of open, closed, slider and multiple-choice questions on a 7-point Likert scale. It focused on the six hypotheses before finishing with the central research question. While the main part of the survey was framed neutrally, we ended with a series of provocative statements to flush out their emotional reaction to the GDPR.

The qualitative analysis of the free text responses was informed by the Braun and Clarke six-step process (2006) and the Williams and Moser art of coding and thematic exploration (2019). The first author coded all the data, following an open-axial-selective coding process. An open, primarily inductive process was used to develop an initial codebook. The codes were discussed and refined

with the second author in weekly meetings. Any inter-coder differences of interpretation were resolved by discussion. This process eventually led to the themes presented in this work. The codebooks and statistical distribution are in Appendix B.1.

The quantitative analysis was executed in Python. The precise statistical tests for each question are described in the Analysis and Results section. The data and reproducible analysis pipeline is available at osf.io[1].

5.2.3 Ethical considerations

The authors' departmental Research Ethics Committee approved this study. The online survey is designed to include pseudonymity, confidentiality and informed consent. The study does not identify individual participants. We do not ask questions that could identify the organisations (or the individuals themselves). The participants were aware of the research's purpose, the researchers involved, and their role in it. Participants were offered compensation at a rate of £10 per hour for participating.

5.3 Analysis and Results

5.3.1 Background demographics

In the final phase #3 of the study, most participants were from large (250 to 2,499 employees) and very large companies (2,500+). The Operations/Manufacturing and Customer Service departments accounted for just over 50% of the sample (see Appendix B.1 for details).

5.3.2 Hypothesis 1: Consumers are aware and knowledgeable about the GDPR

In the larger phase #2 survey, 93% of respondents confirmed awareness of GDPR or the General Data Protection Regulation. Only those who acknowledged familiarity were invited to the subsequent main study.

Regarding the question 'How well do you know what rights GDPR gives you as a consumer?', we employed a slider scale from 0 (nothing) to 100 (expert) for more precise quantification. The average score was 50.6, with a median of 53. Notably, the distribution in Figure 5.1 hints at two distinct populations—one less confident in their GDPR knowledge. A Kolmogorov-Smirnov test supports this, rejecting the null hypothesis of a single normal distribution ($p = 0$, $s = 1.00$).

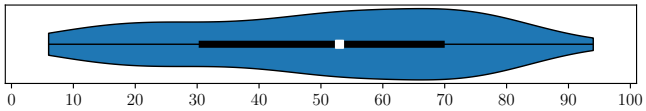


Figure 5.1: Violin plot of participants self-evaluated knowledge of GDPR consumer rights.

[1] https://osf.io/rkvz9/?view_only=5f68dc6f7f4a494fad2ef5f8c6eff862

Respondents were then presented with eight statements, of which four were correct regarding consumer rights, to test their depth of knowledge of the GDPR. The answer options were yes, no or unsure. While the averaged scores per individual are pretty high, only 59% of respondents got all the positive statements correct, and only 20% got all the negative statements correct, i.e. correctly identified the incorrect statements (Figure 5.2).

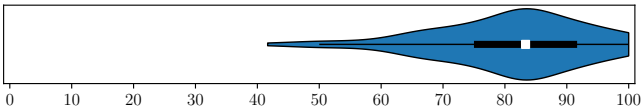


Figure 5.2: Violin plot showing the percentage of questions correctly answered about consumer rights.

We conclude there is a high awareness and knowledge of the GDPR. People may lack confidence that they know their consumer rights under the GDPR at a high level but are more sure-footed at a detailed level. Participants scored high on recognising legitimate rights but were unsure when presented with made-up rights.

5.3.3 Hypothesis 2: Consumers lack awareness and knowledge about the regulator

We assessed consumer awareness of the UK GDPR regulator by repeating questions from the phase #2 survey. Participants were asked to identify the regulator from five possible answer options. In the survey, 38% correctly guessed the Information Commissioner's Office (ICO), and 47% did so in the subsequent main study. Follow-up analysis revealed that those who initially chose the ICO remained consistent, while those who initially selected the DPA options wavered. Overall, we found no significant learning effect. Refer to Table 5.1 for detailed confusion analysis.

Table 5.1: Confusion matrix comparing the participant's guesses for the name of UK's GDPR regulator between the pre- and main-study (which were 8 weeks apart)

Main Study \ Pre Study	The British Privacy Authority (BPA)	The Data Protection Authority (DPA)	The Information Commissioners Office (ICO)	The Office of Data (OfDat)
The Data Protection Agency (DPA)	0.0	20.6	2.9	1.0
The Data Protection Authority (DPA)	0.0	23.5	3.9	0.0
The Information Commissioners Office (ICO)	0.0	12.7	34.3	0.0
The Office of Data (OfDat)	1.0	0.0	0.0	0.0

This was followed by an open question 'What is/are the main purpose(s) of the GDPR regulator?' Table B.2 in the appendix shows a topic analysis performed by two researchers using inductive coding to classify the textual responses. The top four purposes were to monitor companies' compliance, protect data (security), issue fines, and ensure against data misuse.

Next, respondents were asked about the regulator's expected roles from a list of six statements. All of them are true. Table 5.2 shows the results. 29% identified all correct statements, and an additional 30% recognised 5 out of 6.

Table 5.2: Answers to the question 'Which of the following roles is the regulator expected to do?'

Roles of the regulator	No	Unsure	Yes
Give advice to members of the public	10.8%	31.4%	57.8%
Give guidance to companies about their obligations	2.0%	7.8%	90.2%
Maintain a public register of data controllers	3.9%	45.1%	51.0%
Deal with concerns/complaints raised by members of the public	2.0%	8.8%	89.2%
Fine companies for proven data misuse	2.9%	11.8%	85.3%
Fine companies for data breaches	2.0%	13.7%	84.3%

We conducted repeated-measures adjusted chi-squared tests to assess the significance of these results. The first test rejected the idea that responses (Yes / Unsure / No) were randomly distributed (with $p < 10^{-8}$ for all statements). The second set of tests, focusing on Yes / Unsure responses, also showed no statistical significance (with $p < 0.01$) except for 'Maintain a public register of data controllers' ($p = 0.544$).

Approximately 45% of participants reported awareness of companies being fined by the regulator, with no statistically significant correlation found between this awareness and the belief that the regulator should fine companies (Mann-Whitney $U = 5.5$, $p = 0.82$). Interestingly, among those aware of fines, 53% could not recall the identity of the fined companies. Among those who could recall, the top three mentioned were Facebook, British Airways, and Talk Talk (a UK mobile phone operator).

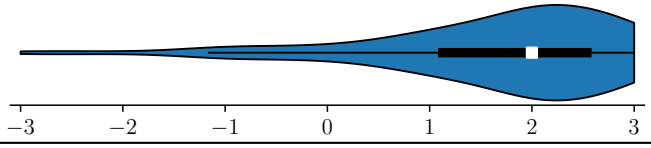
Given less than half could recognise the ICO from a shortlist, we conclude moderate consumer awareness exists regarding the regulator's identity, with slightly higher awareness of its role and actions.

5.3.4 Hypothesis 3: Consumers feel their privacy is better since GDPR was introduced

In different parts of the survey, participants responded to three Likert scale statements related to GDPR (Table 5.3). All of the responses were overwhelmingly positive. No statistically significant relationship was found between these answers and participants' company size or department.

We calculated a composite score for Hypothesis 3 by averaging individual responses (weighted from -3 to +3 based on their position on the Likert scale). The mean composite score is 1.67 with a standard deviation of 1.2. A t-test ($t = 13.94$, $p < 10^{-24}$) confirms that this average significantly differs from a mean of zero. Our conclusion: consumers strongly perceive improved privacy since the introduction of GDPR.

Table 5.3: Questions relating to Hypothesis 3.

H3 Questions	Strongly disagree	Disagree	Mildly disagree	Neither agree or disagree	Mildly agree	Agree	Strongly agree
GDPR means makes me feel more in control of personal my data	2.0%	3.9%	3.9%	14.7%	9.8%	42.2%	23.5%
GDPR is good for the consumer	1.0%	1.0%	1.0%	8.8%	4.9%	46.1%	37.3%
GDPR has improved privacy	1.0%	2.9%	6.9%	9.8%	11.8%	47.1%	20.6%
Aggregate distribution							

5.3.5 Hypothesis 4: Companies have responded to GDPR and made changes

When asked to self-evaluate, 'How well do you know what your company has to do in order to comply with GDPR?' on a slider scale with 0='I know nothing' and 100='I am an expert', the average was 48, the median was 50, and STD was 27 (see Figure 5.3). The distribution appears bimodal, indicating both less knowledgeable and expert individuals. A Kolmogorov-Smirnov test rejects the null hypothesis of a single normal distribution with $p < 10^{-100}$ ($s = 0.95$).

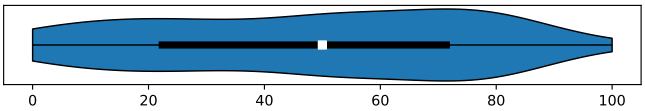


Figure 5.3: Distribution of answers to 'How well do you know what your company has to do in order to comply with GDPR?' on a scale of 0–100.

Respondents were presented with seven statements under the question 'Which of the following are rules that a company must comply with when handling personal data under GDPR?' and asked to answer yes, no or unsure. See Table 5.4 for the results.

We conducted two sets of multiple-comparison adjusted chi-squared tests. The first tested whether responses (Yes/ Unsure/No) could be randomly distributed. This was rejected with $p < 0.001$ for all statements. The second set focused on Yes/Unsure responses, and again, all are statistically significantly different from random apart from 'Must be made available to national security if asked', which has $p = 0.2$. Participants score high on knowledge of individual company obligations, with some uncertainty regarding the national security exemption.

Respondents were offered 10 statements on how their employer company had responded to the GDPR. Table B.4 in the appendix shows the results. Six of these were also asked in the shorter pilot.

We calculated a composite score for observed organisational changes by weighting each individual's response from -3 through to +3 based on their posi-

Table 5.4: Real and made-up rules a company must comply with when handling personal data under GDPR. All obligations bar the 5th are true.

GDPR obligations	No	Unsure	Yes
Fair, lawful and transparent use only	1.0%	4.9%	94.1%
Specific and explicit purpose	6.9%	14.7%	78.4%
Limited to only what is necessary and relevant	5.9%	6.9%	87.3%
Data must be kept up to date	5.9%	14.7%	79.4%
Data can be kept for longer than necessary	74.5%	17.6%	7.8%
Data must be kept safe and secure	1.0%	0.0%	99.0%
Must be made available to national security if asked	13.7%	49.0%	37.3%

tion on the Likert scale (reversing scales as required) and averaging it over the 10 statements. Figure 5.4 displays this distribution, with a mean 0.71, std 1.11. Rejecting the null-hypothesis of a normal distribution with mean of 0 (1 sample t-test with statistic = 6.46, $p < 10^{-8}$), suggests that people have indeed observed changes in behaviour due to the GDPR.

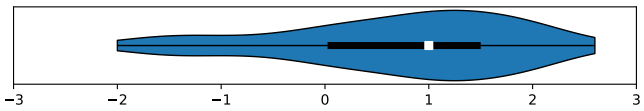


Figure 5.4: Average observed change in the company due to GDPR.

Finally, we compared the scores from the phase 2 pilot and the main study. Figure 5.5 shows a violin plot of the absolute difference in Likert response scores for questions asked in both studies. Wilcoxon signed-rank tests reveal no significant differences ($p < .01$) in participants' responses across repeated questions in the main survey, conducted 8 weeks later. The non-absolute average, with a mean of 0.09, indicated a minimal change in the time between the pilot and the main study. Overall, people's perceptions of changes in their company have remained remarkably stable.

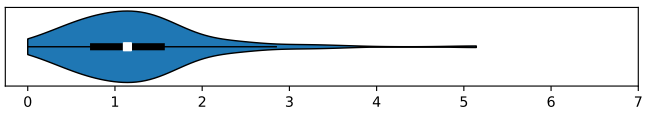


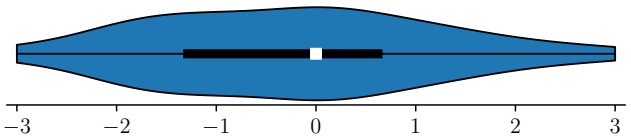
Figure 5.5: Average absolute difference between Likert responses between the pilot and main study for questions relating to observed changes due to the GDPR.

We conclude our sample believes their employers have responded to the GDPR and observed changes. While they may lack confidence that they know GDPR compliance requirements in theory, their high correct scores on specific questions demonstrate knowledge in practice.

5.3.6 Hypothesis 5: Employees lack awareness of the GDPR regulator at work

After ensuring participants knew that the ICO was the UK GDPR regulator, participants were asked to respond to three statements regarding the visibility, reputation and punitive powers of the ICO in their workplace. Table 5.5 shows the questions and results.

Table 5.5: Questions relating to Hypothesis 5: Employee lack awareness of the GDPR regulator at work.

H5 Questions	Strongly disagree	Disagree	Mildly disagree	Neither agree or disagree	Mildly agree	Agree	Strongly agree
The ICO does pop up occasionally in discussions at work	23.5%	25.5%	12.7%	13.7%	13.7%	7.8%	2.9%
In work discussions, the ICO is well regarded	4.9%	10.8%	2.9%	61.8%	6.9%	9.8%	2.9%
Staff have been informed that the company could face big fines by the ICO for data misuse or data breaches	11.8%	11.8%	12.7%	15.7%	7.8%	24.5%	15.7%
Aggregate distribution							

The survey shows that the ICO is not a topic of conversation in the office; people have no opinion about its reputation, but they are aware their employer is liable to fines for data misuse or data breaches. We calculated a composite score for Hypothesis 5 by weighting each individual's response from -3 through to +3 depending on where the answer sat on the Likert scale and averaging it over the three questions. The mean is -0.23 with a standard deviation of 1.41. We cannot reject the null hypothesis that this distribution is drawn from a Normal distribution with mean 0 (one sample t-test with statistic= -1.61, $p = 0.11$). It is possible that participants were answering randomly to this question. We concluded that employee awareness of the GDPR regulator in the office is mixed at best.

5.3.7 Hypothesis 6: Employees have seen little benefits to their company from GDPR.

We analysed this question in three stages: First, we asked participants to what extent their job had changed due to the GDPR, followed by open questions about the advantages and disadvantages of the GDPR. Then, on the next page, participants were asked to what extent they agreed with eight impact statements about the GDPR, and finally, we asked them to judge if the GDPR was good for their company. All answers can be found in Table 5.6, and we will discuss each of the previous parts in turn next.

Initially, participants were fairly evenly split about the effect of the GDPR on their job. This continued to be the case when asked about the advantages

Table 5.6: Questions relating to Hypothesis 6. The second and all subsequent statements are about the impact of GDPR on the respondents company, Questions 2–5 are about negative aspects of GDPR, while questions 6–9 are about positive aspects.

H6 Questions	Strongly disagree	Disagree	Mildly disagree	Neither agree or disagree	Mildly agree	Agree	Strongly agree
The requirements of GDPR have made my job harder and/or more cumbersome	7.8%	22.5%	14.7%	21.6%	25.5%	3.9%	3.9%
Less bureaucracy	11.8%	23.5%	20.6%	36.3%	4.9%	2.0%	1.0%
More compliance costs	1.0%	2.9%	12.7%	33.3%	27.5%	17.6%	4.9%
More cyber-security costs	2.9%	4.9%	4.9%	28.4%	27.5%	25.5%	5.9%
Receive more freedom of information requests	7.8%	11.8%	5.9%	42.2%	9.8%	13.7%	8.8%
Better data security	2.9%	1.0%	2.0%	11.8%	16.7%	52.9%	12.7%
Better awareness of the importance of data privacy practices	2.0%	1.0%	0.0%	16.7%	19.6%	41.2%	19.6%
Less up-to-date customer databases	5.9%	29.4%	20.6%	34.3%	3.9%	3.9%	2.0%
Better trust and confidence in the company brand	2.9%	2.0%	3.9%	38.2%	11.8%	33.3%	7.8%
GDPR is good for my company	0.0%	0.0%	5.9%	28.4%	6.9%	45.1%	13.7%

and disadvantages of the GDPR, where on average, participants agree with mean 0.58 (std = 0.92) that there are negatives to the GDPR, and with mean 1.16 (std = 0.98) that there are positives to the GDPR. Both distributions are statistically significantly different from a normal of mean 0 (with statistics of 6.3 and 12.0, and $p = 10^{-9}$ and $p = 10^{-21}$ respectively). Still, the positives are statistically considerably stronger than the negatives (related samples t-test, statistic $= -4.47$, $p = 2.1 \times 10^{-5}$).

This even split contrasts strongly with the final statement, with almost no participant disagreeing that *GDPR is good for their company*. The ordering may have been a potential biasing factor and/or engaging in the exercise may have helped people to form a more concrete opinion (see also Section 5.4.2).

Through free-text responses, we explored the pros and cons further. First, respondents were asked to identify the biggest disadvantage for their company. Responses (full codebook in the appendix in Table B.5) were categorized into five clusters: no observed disadvantage, increased bureaucratic processes, higher costs, constraints on customer data, and miscellaneous complaints. The most common response was no observed changes or disadvantages, with some attributing this to existing robust processes. The top themes included increased bureaucracy and paperwork, as well as more time-consuming processes. Respondents also mentioned ongoing compliance costs, staff training requirements, and constraints on data collection for marketing purposes as significant drawbacks. Other cited disadvantages included responding to freedom of information requests, internal information sharing difficulties, and uncertainty regarding inadvertent GDPR breaches.

Respondents were asked to identify the biggest advantage of the GDPR for their company. The responses (full codebook in the appendix in Table B.3) can

be categorized into three clusters: better data protection and security, clearer rules, and third, no discernible advantage to their company. Under data protection, respondents linked improved information security and enhanced trust in their company. This applied to client data and their own personal data held by their employer. Some cited transparency and compliance as enhancing their company's brand. Clearer rules led to standardized processes, improved employee training, and better handling of personal data, potentially protecting the company from fines. Some respondents also noted benefits such as the GDPR incentivizing data upkeep, discarding out-of-date information and reducing storage costs.

We conclude people recognise the benefits to their companies but are not blind to the disbenefits of the GDPR.

5.3.8 Research question: GDPR: Is it worth it?

Participants were asked to respond to four statements about GDPR, including the central research question. The overwhelmingly positive responses can be seen in Table 5.7: it appears that when forced to recall and judge the positives and negatives of GPDR, they conclude that it is good not just for them, but also for their employer.

Table 5.7: Questions relating to the main research question: *"do you think it is worth it?"*

H7 Questions	Strongly disagree	Disagree	Mildly disagree	Neither agree or disagree	Mildly agree	Agree	Strongly agree
GDPR means makes me feel more in control of personal my data	2.0%	3.9%	3.9%	14.7%	9.8%	42.2%	23.5%
GDPR is good for the consumer	1.0%	1.0%	1.0%	8.8%	4.9%	46.1%	37.3%
GDPR is good for my company	0.0%	0.0%	5.9%	28.4%	6.9%	45.1%	13.7%
On balance, GDPR is worth it	1.0%	1.0%	4.9%	13.7%	5.9%	50.0%	23.5%

5.3.9 A regression model based on the dual professional-consumer perspective

Given the unique dual perspective of our participants, we explored potential dependencies between our hypotheses. Using 20-fold cross-validated step-wise linear regression models, we identified the smallest set of questions (or composite scores that represent our hypotheses) that maximize model explainability. Our analysis, conducted in Python using scipy and the statsmodels package, can be found in the online supplementary materials. The full regression tables are available in Appendix B.2. Based on this analysis, we propose a new model for understanding the perceptions and influences of the GDPR (Figure 5.6).

We found that consumers' perception of improved privacy (measured through Hypothesis 3) is pivotal for our outcome variables. Several moderating factors influence this view: knowledge of the GDPR (Hypothesis 1), understanding regulator roles (Hypothesis 2), and observing positive impacts on their company due to the GDPR (Hypothesis 6). Our main research question, 'Is GDPR worth

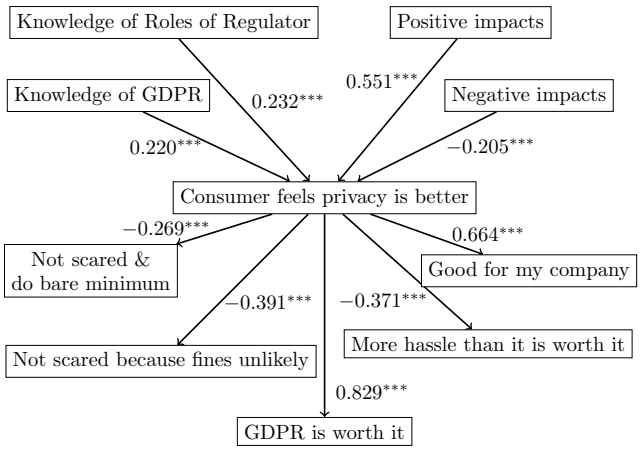


Figure 5.6: Model of our findings, based on 6 regression models (one inputs model, five output models). All coefficients are statistically significant at $p < 0.001$.

it?', is well-explained by a model based solely on 'Consumer feels privacy is better,' achieving an impressive $R^2 = 0.687$. Our participants recognize the impact of GDPR on their privacy and value it accordingly.

5.4 Discussion

This research examined the informed individual's perception of the GDPR. This is important because we can gauge buy-in and learn what works when considering new privacy regulations. Several high-level themes can be drawn from the results:

5.4.1 High consumer awareness and knowledge of the GDPR

The H1 results reveal a strong awareness of GDPR among participants, with 93% acknowledging it in the phase #2 survey, a marked improvement over previous EU surveys. Our research tallies with the literature that people learn about GDPR from news, employer training, and cookie consent notices. Departments like HR, IT, Marketing, and Legal exhibit higher awareness than others, possibly due to its greater impact on their work.

While participants aren't spontaneously confident about their GDPR rights, they recognize consumer rights when prompted. Notably, they understand the right to be informed and the right to request data copies. They are less confident recognising fabricated rights—registering high unsure scores—but that is probably the right reaction. Equally, while participants aren't spontaneously confident about their employer's GDPR compliance obligations, they scored high overall, with the exception of the national security exemption, which is hardly common knowledge.

5.4.2 Respondents lacked a formed opinion

The sequencing of the questions was designed to avoid bias before posing the central research question: 'Is GDPR worth it?' Initially, respondents were hazy about GDPR and its impact on their job. However, once prompted with specific questions about GDPR, the regulator, and observed repercussions at work, they finished the survey with a positive evaluation of GDPR. We speculate participants may default to imprecise gut feelings unless prompted to consider its specific benefits and drawbacks. Future data protection surveys may improve response quality by giving participants the space to develop an opinion.

5.4.3 GDPR has driven changes

The results from H4 prove people have seen changes at work. This shows the GDPR is working. We can be confident the answers are 'solid' because they are very similar to the answers they gave to the same questions two months beforehand in the phase 2 pilot. In particular, they have observed how personal data is handled more carefully, and they have received regular training on the risk of fines due to data misuse or data breaches. More generally, they agreed more than disagreed with all the prompted observed changes. The change that received the highest uncertain score was 'My company collects less personal data than before', but even then, more people agreed than disagreed.

People recognise the upsides (improved data security) and downsides (bureaucracy, time, cost) of these GDPR-driven changes for their employers and for them personally. This latter point regarding cybersecurity tallies with earlier research. However, we bring an original contribution behind how our participants evaluate this. For their employer, people think better information security means less chance of fines. We speculate they may translate this as better job security for themselves. For the employee, better information security makes them feel their own data is handled more carefully by their own employer. We speculate they may project this expectation onto other companies.

5.4.4 Perceptions of privacy have improved

The results for H3 show people feel their privacy is better since the introduction of the GDPR in 2018. This is an important and positive finding since comparative empirical surveys are sparse. The ICO surveys annual changes in trust and confidence scores rather than privacy per se. Other perception research looks at control (Presthus & Sørum, 2021), choice and risk perceptions (Bornschein et al., 2020).

5.4.5 The profile of the regulator may not matter

The results for H2 & H5 show people are not very familiar with the ICO as consumers or as employees. It registers modest name recognition. That said, ICO awareness has improved since the EU Eurobarometer survey in 2019. Back then, only 21% of the UK knew its identity, whereas 38% recognised the ICO in phase #2. People believe its role is twofold—to monitor compliance, including data security and data misuse, and to issue fines. This matches some of the ICO mission statements. People see the ICO as more company-facing and less

consumer-facing. This may not matter since the ICO achieves its objectives via controls through companies. If the people that matter, i.e. DPOs and senior management, rather than ordinary employees are aware of the ICO, then it may not hinder its effectiveness.

5.4.6 Regulator = Enforcer

People's expectation of enforcement is complex. Unlike the enforcer to advisor spectrum outlined in the literature review, the general population have firm expectations of their regulator as an aggressive compliance-led defender of their rights rather than an advice-led consultant to them and their employers. They see the regulator as there to punish and fine non-compliant businesses. However, half of them cannot remember any company being fined. Of the half that could, half could not remember the names of the culprits—so how important are fines really to their perception of the regulator and the regulation? Our regression analysis suggests that people are most likely to believe companies are scared of GDPR fines if they feel privacy has improved because they have observed changes in their own employer and are aware of the compliance obligations of companies.

5.4.7 GDPR is worth it if...

Our regression analysis suggests the following mental models at play: People believe the GDPR is worth it because they feel their privacy is better since the GDPR was introduced. People are most likely to say this if they are confident they know their consumer rights, know the regulator's powers and have observed first-hand the mix of positive and negative changes at work.

People are most likely to think the GDPR is good for their company and not too much hassle if they have seen more positive and fewer negative changes to it and, curiously, are not too knowledgeable of the role of the regulator and the compliance obligations. A sort of goldilocks situation (Wikipedia, 2022): they see more positive than negative changes and don't regard the regulator as too powerful or demanding.

5.4.8 Implications

We examine the implications of these themes across theoretical, managerial, and policymaker/regulator levels.

Theoretically, we question the sustainability of GDPR-inspired changes observed in this study. Will there be compliance decay over time, considering the competition for business focus from newer regulations? The GDPR benefited from massive publicity at launch, but that was five years ago. There are grounds for hope. Recent experiences suggest that EU data regulation often reinforces compliance in other areas, potentially mitigating decay. Additionally, new data protection regulations overseas, inspired by the GDPR, may reinvigorate its relevance.

At a managerial level, our research suggests that constant awareness and knowledge training of the GDPR can lead to unforeseen effects. Raised expectations among employees for high data hygiene practices from their employers

may drive companies to promote their GDPR credentials in order to reassure staff and customers and foster trust in their brand.

Our research also prompts consideration of the optimum positioning for a regulator. If the ICO's focus is primarily on corporate compliance rather than consumer protection, this has implications for policymakers. For instance, should the UK government direct the ICO to issue more fines to reinforce their deterrent effect on corporates?

The positive perception of the GDPR among those who comply and implement it suggests valuable lessons for future policymaking. Incorporating early feedback and buy-in from a dual professional-consumer sample population may enhance the development of new regulations in this field.

5.4.9 Limitations and future work

Participants were recruited via Prolific, which is an on-demand platform for connecting researchers with volunteers worldwide. A major criticism of academics using prolific for surveys is the platform's reliance on convenience sampling, which can lead to a non-representative sample, where participants are primarily motivated by earning money, potentially impacting the quality and reliability of research data due to "survey fatigue" and/or a tendency to provide less thoughtful answers. Participants volunteering for modest payment are unlikely to be drawn from senior management. We attempted to mitigate some of these criticisms by using demographic filters (UK only), careful screening questions, attention checks and up-front information on what was expected.

Although the UK GDPR is virtually identical to the EU GDPR, the findings from a UK-only sample may not be applicable to other EU countries, especially regarding regulator-specific results due to differences in national regulator competencies and resources. As we wanted to ensure non-identifiable responses, we cannot estimate the diversity of companies studied, and there may have been multiple responses from single companies. By expanding the sample size, future work could investigate if participants' views are influenced or different based on their industry sector or country regulator. Since conducting this analysis, the ICO published a survey with a larger sample size than ours, corroborating a subset of our findings with regard to comparable questions. Another research path would be to explore how new complementary data-related regulations reinforce each other and influence consumer perceptions.

5.5 Conclusion

In the UK, GDPR awareness is high, and consumers understand their rights. They perceive improved data protection and personal data control since the introduction of the GDPR. While the regulator's identity awareness is lower, participants recognize its role in upholding rights and imposing fines. This may become a point of dissatisfaction in the long term, as participants struggled to recall companies that had actually been fined.

Interestingly, employees view GDPR as good for their companies because it protects customer data and their personal data. Despite recognizing the overheads (people, process, and technical), they believe GDPR clarifies compliance requirements on their employer and what it has to do to avoid being fined. They

appreciate that their employers (and, by extension, other companies) must be more conscientious in handling and securing personal data. In summary, while GDPR may be viewed as an imposition, participants still think it is worth it. These insights have important implications for policymakers and regulators who may wish to emulate this public support for future regulation roll-outs.

Having explored the positives and negatives of the GDPR for business in Chapter 4 and for the insider-outsider in this chapter, we turn our focus in the next chapter to another critical stakeholder, namely the regulator. Implicit in all our discussions to date is that the regulator has been doing a good job implementing the regulation. In Chapter 6, we explore what "good" means in this context to practitioners and how performance might be assessed more systematically.

Chapter 6

GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved?

6.1 Introduction

Regulation is critical to the working of society. Just as important is how regulators implement it. As society becomes increasingly digitised, privacy regulation and the effectiveness of the regulators executing it will become more pressing.

The European Union (EU) General Data Protection Regulation (GDPR) is regarded as the strongest privacy and security law in the world (even though the word 'privacy' never appears in its text). Although widely studied as a benchmark and blueprint by policymakers when considering a similar regulation beyond the EU, rather less attention has been paid to the actions of the GDPR regulators. Such regulators, known as Data Protection Authorities (DPA), operationalise it in the 27 EU member states, the 3 European Free Trade Association (EFTA) states and the United Kingdom (UK).

Performance measurement of regulators is challenging due to the indirect nature of their involvement. Their desired outcomes, such as consumer or environmental protection, are not theirs to deliver but are realised by the organisations they oversee. Many external factors can be beyond regulators' control, and outcomes often do not become evident for several years. Assessing the performance of GDPR regulators, where the very concept of privacy is contestable, brings added complexity. Differences in national laws, administrative processes and historical engagement with industry mean DPAs come to GDPR from different starting points. Differences in human and financial resources mean that DPAs have varying organisational capacities. And differences in political influences mean DPAs' self-confidence and understanding of their role may differ

significantly between European countries. All these factors contribute to the noticeably different implementations of the GDPR. Metrics, where available, are often defined differently and make comparative analysis problematic. Such complexity may explain the surprising scarcity of prior research.

Nonetheless, if we are to hold data protection regulators accountable and to learn best practices, an assessment framework, however imperfect, is required to score their effectiveness individually and relative to their peers. We have already shown in Section 3.3 (page 58) that existing literature fails to answer what good execution means in this context. In this chapter, we research what practitioners think are the objectives of data protection. Next, we explore novel ways to assess regulator performance more systematically. We investigate the perspectives of those stakeholders closely involved in the regulatory process by surveying 70 Chief Information Security Officers (CISO) and conducting 23 face-to-face structured interviews. The interviewees included informed business executives, lawyers, digital rights activists and 4 national regulators. This has not been attempted before in the security community.

Thus, we ask:

RQ1: How is the effectiveness of the GDPR regulator judged by involved stakeholders?

RQ2: How could we better measure the performance of the GDPR regulator?

We supplement the qualitative analysis with data on national budgets, headcount, complaints, investigations and fines from published EU and DPA annual reports.

It is important to note that data protection and privacy are technically different concepts, explained in more detail in Section 2.2. However, all participants and much of the related literature used these terms interchangeably, and we use them as reported. Data protection originates from the right to privacy. The law and terminology vary outside Europe. For example, in the United States, agencies enforce privacy or data privacy laws. In Europe, DPAs enforce data protection rights. Due to the colloquial conflation of these concepts, DPAs are often informally referred to as "privacy regulators".

Our contributions are:

- We interview and survey a hard-to-reach population of industry practitioners and regulators and thematically analyse how they perceive the role of a regulator and how it informs peoples' evaluation in practice. We find a mismatch between the broad presumed objectives attributed to regulators and the narrow criteria used to judge them in practice. Perception of the regulator's effectiveness is subjective, sanctions-focused and influenced by one's role and responsibilities. Moreover, the independence of regulators, intentionally designed to insulate them from daily politics, raises serious questions of accountability.
- We offer a series of key performance indicators (KPI's) and make structural suggestions around centralised and standardised reporting of cases to deliver improved learning, legitimacy, transparency and comparability. We believe our findings have important implications for the development of future regulator assessment and accountability in Europe and in GDPR-like regimes outside Europe.

The chapter is structured as follows: Section 6.2 describes the methodology. We report our findings in Section 6.3 and show how five broad themes but

narrow criteria emerge in answer to RQ1 and discuss ten potential performance indicators in answer to RQ2. Section 6.4 discusses the findings, and Section 6.5 concludes the chapter.

6.2 Methodology

We used a mix of qualitative and quantitative research approaches based on semi-structured interviews, surveys, and publicly available data to understand, describe and explain how people perceive the success of privacy regulators. We seek to uncover how people conceive what regulators do or should do in terms that are meaningful and that offer rich insight (Banks, 2018). Qualitative research techniques and interpretive analysis have an acknowledged tradition within information systems research (Walsham, 2006). An inductive approach of applied thematic analysis (Guest et al., 2011) was used for the interviews. Quantitative supplemental data was drawn from multiple sources to help contextualise the reported activity of regulators.

6.2.1 Qualitative data collection & analysis

Our research findings are based on 23 semi-structured one-to-one interviews and 70 survey responses conducted between February to April 2023. The study's guiding research questions were "How is the effectiveness of the GDPR regulator judged by involved stakeholders?" and "How could we better measure the performance of the GDPR regulator?" The questions were deliberately broad given the exploratory nature of the study and the absence of previous findings on this subject.

The interview structure underwent two phases before we settled on a protocol to operationalise the RQs. In the initial three interviews, we found that if you led with questions about regulators, participants referred back to the regulation. And if you led with the regulation, participants either claimed unfamiliarity with the legal text or felt that it depended on the regulator. We also found that we had too many questions. Ultimately, to avoid going around in circles, we found that leading with "In your opinion, what are the objectives of the regulator" stimulated practitioners to think holistically about the topic and put them in the right frame of mind for RQ1. We then reflected back to them their answers and asked how they judged or measured regulator effectiveness against their stated objectives.

To answer RQ2, we initially asked participants to suggest other measures. This was not productive. Participants either repeated their answers to RQ1 or went off on tangents. Instead, we discovered we could better focus the interview by presenting them with 10 generic KPIs and inviting them to discuss and rank them in importance. If they didn't volunteer it in conversation, we invited them to create, merge or omit our KPIs to address RQ2 to their satisfaction. The interview protocol can be found in Table C.6 in the Appendix.

To generate the KPIs in the absence of an official EU KPI scorecard, we looked for inspiration in the earlier-referenced literature in Section 3.3. Ideally, if the objective of regulation is to enable governments to drive behaviour change to achieve policy objectives (Black & Kingsford, 2002; National Audit Office, 2021), this meant we needed metrics that evaluated the success of the DPA's in

meeting the technical goals set out in the GDPR and the more intangible expectations of society in general (which is a tall order). We needed to be practical and choose indicators that were measurable and accessible. We also required a range of metrics to track performance across several dimensions. Starting with the theory of input-based regulation (A. Ogus, 2004), we use regulator financial budgets and human resources, accessible in the DPA's annual reports, as an input metric. Adequate resources are generally regarded as an essential prerequisite to good regulation infrastructure. Leaning on the theory of output-based regulation (Joskow & Rose, 1989), we chose activity metrics such as the number of investigations, complaints and fines as most regulators publish them, and they are meaningful to consumers and businesspeople alike. It is not straightforward to apply outcome or risk-based regulation theory (Baldwin et al., 2012; Hahn & Dudley, 2004) in this context since confidence in the regulator and the system is difficult to encapsulate. Although less quantifiable, we chose impact measures such as the media impact of fines and the deterrence effect of large fines on business as they capture the longer-term effects. As perception metrics, we chose public awareness and understanding of GDPR rights and feelings of improved personal data control as key stakeholder measures. Similarly, we chose business perception of good guidance and outreach as the other key stakeholder measure. Together, they follow Coglianese's recent works (Coglianese, 2012) on measuring regulatory performance by evaluating the impact on society and how they affect different groups of people.

Interviews were conducted and recorded over Microsoft Teams as recommended by our organisation's ethics and data protection policies. After transcription, recordings were deleted. The interviews took between 30 minutes and 110 minutes, with an average of 50 minutes. One participant preferred not to be recorded, and two were interviewed in person rather than over Teams, and their data was collected via note-taking. The NVivo 1.7.1 platform was used to code and analyse the text. The analysis was informed by the Braun and Clarke (Braun & Clarke, 2006) six-step process, the Ryan and Bernard (G. W. Ryan & Bernard, 2003) techniques on theme identification and the Williams and Moser (Williams & Moser, 2019) art of coding and thematic exploration. The authors followed an open-axial-selective coding process. It involved both deductive and inductive approaches, where the former produced a set of a-priori codes while the latter produced the final set of themes that we present in the results section. The a-priori codes comprised 10 KPIs and a handful of generic themes for regulator objectives and judgment criteria. All a-priori codes were general and did not include loaded terms. Analysis of the interview transcripts expanded the number of codes, yielding altogether 76 regulator objective codes, 74 judgment criteria codes and 24 KPI codes. Each code had between 1 to 30 snippets of interview text behind it. Through an iterative process, the authors amalgamated similar codes and clustered codes until the final themes began to surface. We do not report inter-rater agreement scores, as they are inappropriate in reflexive TA (Braun & Clarke, 2006). The final codebook can be found in Appendix C.

The survey of the 70 CISOs was conducted over Mentimeter, an audience engagement platform. After a short introduction by the authors, the presentation screen switched to the Menti screen. The survey consisted simply of four questions: "What are the objectives of a privacy regulator, in your opinion?" and "How do you judge the effectiveness/success of a privacy regulator?" The

audience could input their answers via their mobile phones or laptops into a dynamic word cloud and see everyone else's answers as well. The third question presented them with our ten potential KPIs and asked them to rank them. This live and instant polling feature meant they could see the cumulative ranking in real-time. Finally, the fourth question asked "What other KPI measures might be better?" which allowed them to suggest alternative KPIs onto the word cloud. In this way, we collected their input for analysis.

6.2.2 Sample characteristics

We aimed to recruit a diverse range of stakeholders for our privacy and security study, with a particular focus on chief information security officers (CISOs). The author was invited to speak at a confidential invitation-only information security industry meeting organised by a Big 4 consultancy firm for their high-value clients on the 7th of March, 2023. Under Chatham-House rules, we were allowed to mass-test our research questions and KPIs using the Mentimeter presentation and real-time voting platform. We began recruiting for interviews and successfully brought in CISOs, former CISOs, management consultants, and privacy partners from law firms. We contacted NGOs, receiving valuable help and introductions to academics, national regulators, and EU contacts. These introductions proved more effective than approaching the data protection regulators directly. Networking and snowball sampling helped us recruit sales, marketing, data protection and general management professionals from SMEs and international companies, ensuring a diverse perspective. In total, we surveyed 70 CISOs at the private industry meeting and had face-to-face interviews with 16 business people, 3 NGOs and 4 data protection regulators. We categorized them for analysis: Legal (in-house and external lawyers), Executive (non-legal business individuals and consultants), NGO (European and U.S. organizations), and Regulator (EU and EFTA regulators).

Table 6.1: Interviewees P1–P23 & Conference Survey C1–C70

Group	**Labels**	**Male/Female**
CISO	P1 to P6	5/1
Executive	P7 to P10	2/2
Legal	P11 to P16	2/4
NGO	P17 to P19	2/1
Regulator	P20 to P23	4/0
CISO Conference	C1 to C70	64/6

It is worth noting that we did not include consumers in our sample because we wanted to interview individuals who were involved in the regulatory process. Earlier work by the author, as described in Chapter 5, found inter alia that the UK data protection regulator registered modest name recognition with a UK-based sample. Ordinary people do not spend time thinking about our research question topics. For this reason, we felt recruiting NGO's who were full-time consumer digital rights advocates would be more productive in capturing the user perspective.

6.2.3 Quantitative data collection & analysis

There is no one central database of GDPR regulator activity. Instead, one has to sew together information from diverse sources.

The EDPB publishes a register containing decisions taken by national supervisory authorities following the One-Stop-Shop cooperation procedure (Art. 60 GDPR) on its website. This is a small subset of all decisions. The EDPB has also published two overviews of resources made available by Member States to the DPAs (EDPB, 2021, 2022). These contain data on financial and human resources and enforcement statistics. The 2022 overview is shorter than the 2021 overview and is light on detail. Nevertheless, these two documents are useful.

The NGO, noyb, maintains a GDPRhub Decision Database (noyb, 2023a). Volunteers collect summaries of decisions by national DPAs and courts in English. It is incomplete because not every DPA issues its reports publicly. This is a limitation of this analysis. The European law firm CMA maintains a database (CMS Germany, 2023), Enforcement Tracker, which tracks similar data.

The EDPB, EDPS and the DPAs all publish annual reports. There is no standardised format. They are all different. There are no harmonised definitions for cases or decisions which make comparative analysis problematic. Despite these limitations, we use the data from the referenced sources to complement and augment the qualitative analysis.

6.2.4 Ethical considerations

The study was approved by the authors' departmental Research Ethics Committee and is designed to follow the principles of pseudonymity, confidentiality and informed consent. Individual participants are not identified and were not compensated. The participants were aware of the research's purpose, the researchers involved, and their role in it.

6.3 Results

Section 6.3.1 is an overview of the financial, human resources and activity data of the GDPR regulators. Although incomplete, it sets the scene for appreciating the five themes that arose when participants were asked how they currently judge the effectiveness of a privacy regulator in Section 6.3.2 and appreciating the relevance of the KPIs that were discussed as potentially better measures of performance in Section 6.3.3.

6.3.1 Regulator data

As discussed in Section 6.2.3, regulator data is not centralised. Table 6.2 has been assembled from multiple sources with differing time cut-offs. We did request data up to the 5th anniversary of GDPR from all 31 DPAs but only 13 had replied after six weeks (5 referred to us their out-of-date and/or incomplete websites, 5 sent acknowledgements with no follow-up, and 3 supplied full answers).

Germany and the UK have the biggest budgets and headcounts but are not the biggest finers by number or value. At least ten DPAs still have budgets under €2m. The Irish DPC is the "lead" authority for Google (including YouTube), Meta (including Facebook, Instagram, WhatsApp), Apple, TikTok, and Microsoft (including Linkedin, Xbox, etc.) across the EU, because these firms have their European headquarters in Ireland. This explains why it is the lead enforcer in terms of fine value and cross-border cases (Gentile & Lynskey, 2022). Its budget is not the biggest, but it is in the top 5 and almost level with France. The world's fourth technology firm by market capitalisation, Amazon, is based in Luxembourg. After a recent decision, its regulator is now the second-highest finer by value. The Spanish regulator, by far and away, remains the most active enforcer as measured by the number of fines, followed by Italy and Romania.

6.3.2 RQ1: 'How is the effectiveness of the GDPR regulator judged by involved stakeholders?'

As described in the Methods section, we broke this into two parts. First, we asked 'What are the objectives of the privacy regulator, in your opinion?' because practitioners tied themselves in knots pondering the purpose of the regulation. Unsurprisingly, apart from a subset of legally trained participants, most practitioners were unaware that the purpose of the GDPR is clearly described in its text in Article 1 (EU, 2018b), and the role and responsibilities of supervisory authorities are described in Article 57 (EU, 2018d). Next, once they were focussed on how they construct the purpose of the regulator in their own minds, we followed up with, 'How do you judge the effectiveness/success of the privacy regulator?'

In summary, our research has identified five themes that capture how practitioners perceive the role of a privacy regulator and how it informs their subsequent evaluation thereof. The first two refer to a collection of related perceptions that we have clustered under the portmanteau of Lofty Views and Cynical Views. The other three are Enforcement, Clear Guidance for Business and Consumer Protector. We find judgement is very much in the eye of the beholder, depending on the expertise and background of interviewees. Each group (CISO, NGO etc.) had a different mental scorecard for evaluating regulators. We also find that the criteria they use in practice are a small subset of the many objectives they cited for the first part of RQ1.

The following sections will discuss each theme and how practitioners evaluate them to answer both parts of RQ1. The codebook for each theme can be found in the appendix C.

6.3.2.1 Lofty view

The lofty or idealistic view is that the regulator is there to be a change agent and execute many of the technical justifications outlined in Section 3.3.1. Thus, the regulator was there to ensure the regulation was a priority in organisations, that executives took responsibility and that it resulted in *"ex-ante good behaviour rather than ex-post fines"* (P9). Without using the words 'market failure', practitioners instinctively saw the regulator as there to make the rules

Table 6.2: GDPR Statistics

Country	Budget[α β]	FTEs [β]	Cases[γ]	Complaints[γ]	Investigate[γ]	Fine Num[δ]	Fine Val €[ϵ]
Austria[ζ]	4.6m	45	1940	1822	337	20	25m
Belgium	9.7m	62	1370	1368	2	39	1.8m
Bulgaria	1.9m	87	274	445	133	24	3.7m
Croatia[η]	1.39m	34				20	2.8m
Rep of Cyprus	0.8m	23	19	9	3	37	1.36m
Czech Rep	6.4m	113	916	687	45	26	0.17m
Denmark	7.8m	80	5726	1328	100	25	2.4m
Estonia	0.9m	21	511	416	28	6	0.3m
Finland	4.5m	52		1527	22	18	2.6m
France	23.9m	263	3630	5830	162	35	298m
Germany[κ θ]	114m	1155	17616	8089		149	55m
Greece	2.5m	51	519	428	6	57	30.6m
Hungary	4m	111	174	50	10	68	2.3m
Ireland	23.2m	257	7400	1700	5	24	1310m
Italy[θ]	44.6m	139	4896		10	265	123m
Latvia	1.4m	34	462	449		15	0.2m
Lithuania	1.6m	56	3214	555	16	9	0.25m
Luxembourg	8.3m	54	18	176	18	31	746m
Malta	0.6m	14	37	229	1	11	0.36m
Netherlands	28.7m	167	6740	1090	8	22	14.7m
Poland	9.1m	260	4755	3902	31	50	3.4m
Portugal[θ]	2.5m	26				7	6.1m
Romania	1m	34	288	1733	133	138	0.7m
Slovakia	1.7m	45	352	568	9	9	0.13m
Slovenia	2.5m	49	666	257	37	0	0
Spain	16.8m	185	11212	4910	2	646	59.5m
Sweden	11.9m	122	24	943	24	22	14.7m
Iceland	2.2m	19	145	51	6	9	0.2m
Liechtenstein	1.2m	7	30	28	2	1	0.04m
Norway[θ]	7.5m	62	3200			50	10.4m
UK[ι]	66m	823	36343		474	13	75m

Notes: [α] All budgets in € except the UK (£). [β] Budgets and FTE sourced from EDPB Report 5th September 2022 (EDPB, 2022) and UK ICO Annual Report 2021/22 (The Information Commissioners Office, 2022). [γ] Cumulative cases, complaints and ex officio investigations sourced from EDPB Report August 2021 (EDPB, 2021). [δ] Cumulative number of publicly available fines up to 16th May 2023 sourced from CMS GDPR Enforcement (CMS Germany, 2023). [ϵ] Cumulative value of known fines (which does not include all fines as some DPAs do not identify the controller or quantify the fines) up to 16th May 2023 sourced from CMS GDPR Enforcement (CMS Germany, 2023). [ζ] Austrian data replicated from 2020 as there was no data for the 2021 report. [η] Croatia's GDPR did not formally come into force until January 2023. [θ] Data is missing from EDPB report. [ι] UK budget figure is not exclusive to GDPR duties and cases include complaints and data breaches. [κ] German records are only available from some of their regional SAs.

for everyone and *"create a trustworthy market"* (C7). A common presumption was that the regulator should be independent, impartial and proportionate.

How practitioners evaluated this aspiration, however, was indeterminate. Success was judged by intangibles such as leadership, vision, and being seen to take a balanced multi-stakeholder approach to issues. Appearances that showed they were monitoring and in control were important. Being accessible and an organisation capable of learning were also quoted as good markers of effectiveness.

6.3.2.2 Cynical view

There is a sceptical or cynical view that the regulator is there to appear to be in control. *"If you don't control and you're not seen to control, then what's the point"* (P6)? Non-regulator participants believed the regulators' organisational agenda was to look good and always plead insufficient resources. NGOs believed regulators were complicit in *"compliance theatre"* (P18). One regulator accused a fellow regulator of *"indulging in procedural rather substantive activities"* (P22). He felt his fellow regulators *"were deliberately secretive as a group"* (P22). This chimed with another pan-European regulator's observation that *"We have KPIs but the definitions are not consistent. We have reports but not from all member state regulators"* (P23). The personal agenda of staff was assumed to be to gain experience or serve a term and then parachute into a better-paying job in a corporate or a consultancy.

This negative view coloured how participants evaluated regulators in practice. For some, the measure of success was *"a reduction in the number of data breaches"* (C3) or *"a lack of news about breaches"* (P8) or *"a lack of enforcements"* (P8). Expressed slightly differently it was *"less fines, but without consumers complaining"* (C7). That latter sarcastic standard was rationalised as evidence that regulators had succeeded in changing the behaviour of organisations. More prosaically, one participant saw success as eliminating *"people cold call calling you"* and *"spam"* (P7).

6.3.2.3 Enforcer

The enforcement theme emerged as the key role of the regulator. The purpose of a regulator is *"to enforce the law"* (C3) and *"investigate reported data breaches"* (C5). The GDPR was seen to have given regulators *"real teeth"* (P2) to punish companies. Many expressed fear of the reputational impact as much as the financial impact on their company. In fact,

> *"naming and shaming is considered an additional sanction on top of fines by regulators in some EU jurisdictions e.g. Germany."*
>
> (P22)

When practitioners think about enforcement, they think in numbers: *"by total fines issued"* (C8), *"on the number/value of enforcement activity"* (C3), *"the number of complaints"* (P22), *"number of investigations, number of decision, number of corrective measures"* (P19) and *"how many companies have DPOs"* (P1)? When invited to distinguish between their personal and business perspectives, participants see fines as the consummation of consumer protection.

A few thought fines were the wrong thing to focus on and could be counter-productive. Far better to quietly reprimand a company *"rather than putting a head on a spike"* (P5). Some thought fines were a bad measure since an uptick could mean many things: for example, a deterioration in compliance, an increase in regulator resources, a new focus by the regulator or a knock-on effect from events in another country. Some thought fines should be graded in severity depending on whether they were *"sins of omission or commission"* (P4). One CISO felt business was more the victim than the villain since consumers get compensated if they suffer a loss from a data breach whereas the company gets fined and then has to find the funds to improve their information security infrastructure. NGO's, on the other hand, felt fines were not enough to stop certain practices. It is *"the sanctioning power that matters, it's the ability to ban processing. [...] You're selling this data on really. Stop doing that"* (P18).

6.3.2.4 Guide

Education and awareness-raising were cited by all participants, including the regulators themselves. Clear guidance was seen by business people, legal counsel and management consultancies as the primary task of the regulator. Certainty was seen as a shield against inadvertent non-compliance by an organisation.

Judgement of their performance depended on one's interaction and point of view. According to the privacy practice leader at a leading law firm:

> *"the key ingredients are clear expectations through good guidance [...] having a dialogue and relationship [...] guidance which matches the real world problems and anticipates where the tension points are going to be."* (P15)

The educational and informational role was judged by CISOs and DPOs by the visibility of the regulator at industry events and the quality of the information, such as case studies, opinions, codes of practice and FAQs on their website. CISOs, in particular, wanted to see the regulator as a 'collaborator' (P6) and 'partner' and staffed with high-calibre professionals who are *"not just making knee-jerk decisions"* (P2). A management consultant said *"We rely totally on the ICO"* (P9), but certainty is fragile. When Equifax successfully challenged the ICOs ruling in an appeals tribunal, it introduced *"a new level of uncertainty [concerning the solidity of their guidance]. One got to look behind the curtain of the Wizard of Oz"* (P15). When the ICO announced a £180m+ fine on BA but later settled for a fraction of that, a lawyer opined *"they should have gone for something smaller but more solid because any climbdown just makes people believe less that it really does have a big stick"* (P15).

6.3.2.5 Protector

The consumer protection role meant most participants saw the regulator as the backstop, the helper, the adviser, the educator, the body that empowered the consumer, that responded to complaints and launched investigations and protected our privacy. It did not come up in the interviews, but it is worth noting the protection role is also vital for people beyond just consumers (e.g. workers, students, citizens, refugees).

This expectation of the regulator suffered the same lack of follow-through as the lofty view. Participants spoke generically about the regulator helping the public if they had concerns but failed to quote anything tangible. Complaint metrics were mentioned by a few but in a dismissive way. One NGO was more interested in decisions and corrective actions, as complaint volumes could be shaped as much by awareness as by a lack of awareness and was deemed meaningless. A regulator quoted Article 57 1(f), which refers to the compliant reporting guidelines for regulators, and commented that every regulator did it differently regarding transparency, thresholds, backlogs and case count criteria.

Finally, even the research question itself threw up strange reactions. More than one participant admitted it had never occurred to them to think the question, whilst two legal participants thought it almost bad manners 'to judge the judges'. One NGO joked that the legal profession was so obsessed with ticking boxes that asking them for an opinion about its value was akin to *"asking cattle farmers about veganism"* (P18).

6.3.3 RQ2: 'How could we better measure the performance of the GDPR regulator?'

We found early participants struggled to move beyond their answers to RQ1 or went off on tangents about the regulation itself. To bring better focus to the interviews, we devised a balanced scorecard of ten KPIs that we adapted from work in related fields (Coglianese, 2012; National Audit Office, 2016). We invited participants to discuss them, rank them in importance and suggest alternatives. Separately, we invited CISO's at an information security conference to rank the KPIs. Their ranking was similar with the proviso that the interviewees emphasised the importance of financial and human resources. This section reports the findings under each KPI, suggested alternative KPIs and the two ranking exercises.

6.3.3.1 Secured adequate financial and human resources

Most participants were unsympathetic. *"I'm a bit cynical [. . .] I don't have the right budget and human resources, but I'm still expected to do my job"* (P11). Another opined, *"It's the human default in business to try and get more money and more people to make everyone's life easier"* (P8). In contrast, a regulator said *"75 to 85% of regulators do not have sufficient resources and are forced to prioritise"* (P22). This tallies with the EDPB's 2021 & 2022 overview on resources made available by member states (EDPB, 2021, 2022), which showed 82% and 77% respectively of regulators felt they had insufficient allocated budgets and 86% and 87% insufficient human resources to carry out their tasks. To put numbers to this, the combined budget of EEA DPAs (UK excluded) has grown since 2016, from €167.1 million to €337.6 million in 2022 (Irish Council for Civil Liberties, 2023).

Quality of staff was mentioned often. One CISO, who had been an expert witness in a case, likened it to watching undergraduate regulator staff up against PhD-calibre corporate opponents (P4). There was sympathy for *"overstretched"* (P16) resources although pragmatism ruled

"you are probably never gonna have the level of resources to un-

> *dertake the volume of investigations, complaints and fines that you possibly could get involved with. And so I think you have to pick and choose."* (P5)

However, as the interviews progressed, participants admitted that *"if you want it to be done right, then you have to spend the money"* (P7) and one needs *"adequate financial resources because everything else does come off that"* (P15). In fact, one interviewee took comfort that public statements from the Irish regulator demonstrated they were *"tooling themselves up to have the right resources"* (P11). Regulators have a more nuanced perspective. One thought it was a good KPI because it was a measure of the success of *"shouting or lobbying"* (P22) by a regulator to secure adequate funding, whilst another recognised that the complicating factor of independence meant that *"it's very difficult to make to budget allocation policy-neutral"* (P21).

6.3.3.2 Public perception of improved personal data control

The 70 survey respondents thought this was the most important KPI. Many felt it should be combined or paired with the awareness & understanding KPI as they were intertwined. One regulator liked the emphasis on public stakeholder KPIs. After all, *"DPAs are there for the people"* and *"we are not working for ourselves"* (P22). Active visible enforcement was seen as vital.

> *"I would say that for the perception to be real, it does need some element of public enforcement and a sort of lived experience of the regulator intervening effectively to dissuade the infractions."* (P15)

While there was consensus about the outcome, there was less agreement about the calculation.

> *"If we can contribute to them getting better control of their personal data or personal information, I think we play a good role. How measurable is this is extremely difficult."* (P21)

A second regulator was even more scathing:

> *"Perceptions of it can be your perception of it [...] or the regulated organization's perception of it or the general public's perception of it, and what you will measure there will depend on the year when you're doing the survey."* (P20)

A DPO described it as *"a hygiene factor. People's feelings are not a reliable measure"* (P10).

6.3.3.3 Business perception of good guidance and outreach

When interviewees were asked their views as private citizens, the improved personal control KPI was most important. As business people, however, the relationship with the regulator was more important, as was the perception that it should be there as a partner and collaborator and performing not just a *"auditing policing role [...] but actually contributing and helping you"* (P2). Many felt

this was a good measure as business is an important stakeholder and a *"good judge of character"* (P3). There was generalised grumbling about generic versus specific advice by the legal participants. *"For us, it's clear guidance. So, when we ask a question, we want an answer. We don't want an obfuscation"* (P9). At least two complimented the UK regulator, the ICO, for clear guidance and an informative website. Certainty is key for the advisory profession. *"The purpose of good regulation is to create guard rails"* (P9) so that they can advise their clients on how to operate lawfully. The regulators also have their own reasons for issuing clear guidance. Any room for misinterpretation could undermine *"robust enforcement decisions"* (P20). This tension was characterised as follows:

> *"It's a very complex relationship between a regulator and a company. We want to work together. We both want to achieve the same goal. But at the end of the day businesses are accountable for what they do, and [...] we are controlling them, we are supervising them, so the relationship is not balanced."* (P21)

Another regulator observed *"Most businesses want to comply"* (P22) which is why this metric is important for governance regimes that rely on cooperation.

6.3.3.4 Media impact of fines and regulator leadership

There was unanimous agreement on two aspects: *"the media impact draws attention to the fact that the regulators are taking action"* (P14) and that companies are *"more worried about the public reputational impact than the actual number"* (P2). Even when the fine appears high, *"it's in the headline rather than the bottom line"* (P2). This attitude is probably conditioned by the size of the fines levied historically being small compared to the profits of large multinationals. One NGO wryly characterised the financial pain of €100m+ fines on Meta as equivalent to mere *"parking tickets"* (P18). (This interview took place before the Irish DPC levied a €1.2Bn fine on Meta in May 2023, the first and only fine to date to breach the Bn threshold).

Public fining of well-known companies in the same industry does however have wider effects and *"everybody will sit up and take note"* (P7). Quite a few believed that the media impact was linked to the size of the fine. If the press fails to pick up on it and report it, then *"we all know that nothing happens unless there's some media outrage"* (P8). A regulator saw the media impact *"as a means to an end and not the goal itself"* (P22). Another regulator felt fines are enormously important for the perception of their authority that they will *"impose fines on a regular basis when people or when companies or organizations are infringing the law"* (P21). Large fines and associated publicity were seen as important *"game changers"* (P20) because they set an important precedent *"not only at the national level but also possibly at European or global level"* (P20). Leadership was referenced by only one NGO with decades of experience dealing with regulators, and they felt the importance of the *"vision"* (P17) of the CEO was undervalued.

6.3.3.5 Perception regulator is independent of the government

The initial reaction of non-regulators and regulators alike was that it was not a priority. A fairly typical reaction was summed up by one CFO: *"most people*

would not know or care" (P8). All the regulators thought it was a non-issue. For example: *"there's a lot of assurance, at least in the privacy world that the regulator is independent of the government. This is enshrined in the texts and at least in many EU countries, there's a long history of independent regulators"* (P20). When pressed on why it was so unimportant, some commercial participants rewound their initial dismissal. Independence from the government in power is important to business because business doesn't want *"surprises"* or suffer *"collateral damage"* (P2) if regulatory change becomes *"politically expedient"* (P7). In a UK context, some felt the new draft Data Protection Bill showed the ICO wanted to be *"more closely aligned to the government"* (P14) and that concerns *"might bubble up more post-Brexit if the UK [. . .] is playing footloose with your data because they are going after the commercial big bucks"* (P2). In a slightly backhanded compliment, one executive drew comfort that the ICO was more independent than longer established regulators such as telecoms because it was not as well *"connected"* (P5) to business.

6.3.3.6 Good public awareness & understanding of GDPR rights

Everybody interviewed, apart from one DPO, thought awareness of GDPR was high. Some questioned *"if the awareness translates into an understanding of the rights"* (P11). For example

> *"subject access requests are a nuisance for lots of organizations. Sometimes they're a nuisance because people request stuff they're not entitled to, which is an education thing."* (P5)

Awareness was regarded as important *"because if you haven't made society aware of what you're doing and taking them with you so that you're working with them, then I think that's a failure"* (P2) as was understanding since *"I think it's paired because if those two are pulled apart, that would be a regulatory failure"* (P2). Education was seen as a key function of a DPA by a DPA because *"better citizen awareness will affect policymaking"* (P22).

6.3.3.7 Fines issued on a scale that deter

A typical endorsement of the deterrence effect is that large fines *"build confidence in the public that actually these guys have teeth. And there's a crossover between fines and the media impact"* (P7). As a DPO put it *"if a parking fine were £1, people would park everywhere"* (P10). For the same DPO, the bigger the headline fine, the better the attention it commanded *"this is the one thing we can hold up [to the board] and say, You know what, if you don't do this, this is what this is the bad thing that can happen"* (P1). Some participants quibbled the fines in the UK were not re-invested, that strict compliance could put the UK at a competitive disadvantage to China, that large fines could cripple the UK economy, that companies weigh up the fines against the commercial benefit of non-compliance, that fines should be commensurate with the harm and that the focus should be less on the stick and more on clearer guidance. The NGOs felt *"the sanctioning power that matters is the ability to ban processing"* (P18).

6.3.3.8 Number of investigations

Regulators were the biggest fans of this metric:

> *"You want to show your performance [...] These are things that [...] we systematically put forward in the annual report because they're key numbers. Those tables over time that you can easily measure do not depend on the people surveyed and things like that."* (P20)

Business people were less convinced. They felt they were *"too open to manipulation"* (P8) and *"more about the performance of the regulator as opposed to whether they are effectively regulating, which is a different question"* (P16).

The NGO's were even more cynical. They regard the metric per se as very important, but they derided regulator-initiated ex-officio investigation metrics. They claimed most were driven by them and by their threats to embarrass the regulators' inaction in the press. *"These people have procedure, political will, resources. Who knows? Some DPAs are definitely quicker than others and we know which ones now after five years if we want a quick decision"* (P19).

6.3.3.9 Number of complaints

The reaction to this metric fell between nice-to-know and downright misleading. A few felt it acted as a good statistical barometer, particularly if it was accompanied by contextual information to add colour. A strong majority questioned its meaningfulness:

> *"I don't know if she's making that sound like it's a positive thing that we've had more complaints or you could actually say that that's because there's greater public awareness. [...] I don't think the number of complaints is a particularly helpful metric, because what's that really showing?"* (P11)

Some accused dissatisfied consumers or disgruntled employees of being opportunistic *"ambulance chasers"* (P2) and using SARs as to further their grievances. One regulator admitted *"it's actually quite tricky to compare the annual reports"* (P21) because *"the notion of complaint, although it is written down in the GDPR is nevertheless not interpreted the same way in every country"* (P21). For example, some regulators are required by national law to respond by letter to every complaint, some push people towards information requests for mediation etc. to stay out of the formal complaint rule process, and others have the discretion to pick and choose what they follow up. One regulator (P22) felt the number of complaints speaks more to awareness of rights and a culture of compliance. If people know their rights, more will complain. The complaints may be justified. Alternatively, people may misunderstand their rights and still make complaints. Different countries will have different thresholds for reaching out and trusting their authorities. For example, he believes that data breaches are over-reported in certain countries. By contrast, in other countries, the complaint procedure can be formal and complex. Thus *"this metric could be about how easy it is to lodge a complaint"* (P22).

6.3.3.10 Number of fines

This was controversial. Regulators like this metric: *"You will focus [...] on the things you can measure [...] it's important for our own work as a KPI"* (P20). There was broad agreement among regulators that the desired outcome, i.e.

behavior change, was more important than the fine per se. One lawyer applauded the ICO shift to *"naming and shaming as they were in slapping people with big fines"* (P16). Another lawyer liked *"more regulators showing their teeth [...] particularly in Europe, you're seeing Spanish, Italian DPA's issuing a lot of fines, but small amounts not sufficient to deter, but maybe to make people think twice"* (P14). However, many were sceptical of the integrity of the metric since it was generated by the regulators themselves. Liking it to the boundaries of hospital waiting times or flight times being changed to meet a scheduled target, more than one cynic felt regulators would *"spin the number to suit the argument"* (P7). One regulator even accused another of being guilty of that gamesmanship rather than focusing on substance.

6.3.4 KPI rankings

Table 6.3: Average Ranking scores of KPIs for Interviews (I) and CISO Menti (M) responses. The lower the rank (the darker the colour), the more important.

KPI	I	M
Secured adequate financial and human resources	2.7	6.3
Public perception of improved personal data control	2.8	2.7
Business perception of good guidance and outreach	1.8	4.5
Media impact of fines and regulator leadership	3.9	6.9
Perception regulator is independent of the government	4.5	5.3
Good public awareness & understanding of GDPR rights	2.7	3.4
Fines issued on a scale that deter	4.8	6.5
Number of investigations	5.1	5.1
Number of complaints	5.8	6.8
Number of fines	5.4	7.4

Table 6.3 shows the interview results in one column and the Menti survey results in the other. At the end of each interview, participants were asked to rank the KPIs in importance. When their votes were aggregated, they ranked business guidance as the most important evaluation KPI (which may be influenced by the business majority of the sample). The two public perception metrics combined with budgetary sufficiency were ranked collectively in second place. Separately, the Menti rankings were collected from attendees on the Mentimeter survey platform after our presentation at an information security conference. They show the two public perception KPIs as preeminent and then business guidance KPI. The slight difference in ranking may be due to the discretion interviewees took to cluster KPIs, whereas the survey platform enforced a strict individual KPI ranking on the Menti voters. It may also be due to the interviewees' freedom to discuss a topic such as budgets, whereas the conference attendees did not have that interactive option. Nonetheless, the top three KPIs are the same in both surveys.

6.3.5 Alternative KPIs

The two most common alternative KPI themes were regulator responsiveness and regulator accountability. Annual reports were characterised as backwards-looking:

> *"If they set forward-looking goals and targets and then had to report back on whether they achieved those. I think it would make them more accountable."* (P11)

The NGOs wanted more granular data on the pipeline of cases, the stage of each case, and the turnaround times for a decision (European Digital Rights, 2022; noyb, 2022). They wanted transparency of the in-and-outflow balance of cases to reveal backlogs and a measure of powers exercised, such as decisions, ex officio investigations, dawn raids, and stop orders. One regulator volunteered that one KPI should be about how DPAs proactively investigate risks invisible to the common man, such as invasive ad tech or privacy-destroying AI. To counter the objection that measuring a Hidden Risks KPI may be impracticable, he suggested *"a possible proxy there would be, what about NGOs, expert organizations and bodies? How they perceive the state of play?"* (P22) as part of a stakeholder perception measure. Other ideas included having comparative benchmarks across Europe, a root cause repetition metric to measure recurring systematic violations, and a class action and civil claims metric that was an adjunct to the formal complaint metric.

6.4 Discussion

In this section, we will explore why the indefinable effectiveness of privacy regulators is tied up with the difficulty practitioners have in specifying the regulator's raison d'etre in the first place and how that affects their instinctual evaluations of their performance. We examine the independence and accountability conundrum that is common to many regulators and how it is made worse by the national definitional and procedural differences for a supposedly common regulation like the GDPR across Europe. We identify some basic systems and informational infrastructure that would support enhanced reporting before finally fleshing out a series of KPIs that could form the basis of a framework for individual and cross-country regulator performance assessment.

6.4.1 The indefinable effectiveness paradox

We term it a paradox because just as the privacy paradox (Acquisti, 2004; Spiekermann et al., 2001) is the observed phenomenon that describes the discrepancy between users' expressed concern and actual behaviour regarding online privacy practices, our research indicates there is an analogous paradox that describes the discrepancy between the expressed objectives and the actual criteria practitioners use to judge the effectiveness of privacy regulators. The results of RQ1 show that practitioners hold a wide spectrum of expectations of a regulator spanning the five themes but only have tangible output measures for a narrow subset of those expectations to judge them in practice (i.e. the Enforcer expectation). The results of RQ2 show practitioners revert to higher level goals when given more information and time to consider a range of KPIs. We surmise it is partly due to definitional difficulty and partly due to one's point of view. In political science, it might be characterised as "where you stand depends on where you sit".

Trying to pin down the concept of privacy has challenged philosophers and scholars for millennia (Holvast, 2007; Nissenbaum, 2009; Solove, 2006). As one

regulator put it *"privacy is a fluffy, immeasurable objective"* (P18), which means assessing their effectiveness is problematic if attainment resists definition. As the EDPS puts it "The notion of data protection originates from the right to privacy and both are instrumental in preserving and promoting fundamental rights and values".

Lacking well-defined objectives, practitioners ascribe goals based on their personal motivations and experience. Thus, consumers think about complaint handling, high-profile data breaches and fines, whereas business people think about the clarity of guidance they receive and the calibre of personnel they encounter at the regulator. NGOs prioritise evidence of activity and responsiveness, whereas regulators stress consumer awareness and treasure their independence.

This mismatch has practical implications for regulators around how they frame and communicate their role, prioritise their workload, and thereby demonstrate their value and effectiveness.

6.4.2 The independence-accountability enigma

In Sections 3.3.2 and 3.3.3 we summarised the importance of protecting regulator independence. Our research confirms that the SAs believe they enjoy a high degree of autonomy and business does not see it as a concern. In the course of our interviews, we learnt firsthand of instances where regulators 'lean' on a fellow regulator at EDPB meetings if they think they are being too lenient, for example, but accountability is mainly restricted to an annual report to parliament or to an annual hearing or meeting with the government minister that has administrative responsibility. Whilst an obvious lever, politicians are careful not to be seen to use budgetary decisions as indirect accountability instruments. The EC has started to require bimonthly reports on cross-border cases (European Commission, 2023), but that is the limit of scrutiny. Meanwhile, in June 2023, the Irish Parliament has introduced a new law (Section 26A which modifies the 2018 DPA Act) (Éireann, 2023; Oireachtas, 2023) that prohibits the disclosure of confidential information which the DPC justifies as protecting the integrity of their decision-making process but which the NGOs characterize as a gagging order (International, 2023; noyb, 2023b; Sawers, 2023). There is no provision in Section 26 that allows a third party to audit if the imposition of this new power by the DPC is proportionate or justified. In effect, GDPR regulators continue to mark their homework. Apart from longer-term court challenges, the feedback loop with society seems weak if regulators are immune from pushback.

6.4.3 Practical steps to better accountability

In political science, it is contested that regulators generally face a legitimisation and democratic deficit problem (Maggetti, 2010). Trade-offs exist concerning the simultaneous delivery of autonomy, performance and accountability. Although we make no claim to legal expertise, two alternative sources of legitimacy emerge from our research: the positive evaluation of regulatory performance by all stakeholders (consumers, business and expert organisations) and a procedural component in formalising how GDPR regulators peer-review one another.

To enable this evaluation, one needs a level playing field. A surprising finding was that there exists no central database. At the very least, a common platform

seems like a sine qua non to enable analysis. A second surprising finding was the lack of similarity in reporting styles. Harmonising the format of the DPA annual reports seems an easy win. Given our research revealed a high degree of cynicism regarding 'spin' in annual reports, there may be a role for an EU third-party to audit the data. A third surprising finding was that there exists no EU-wide agreement on what constitutes a final complaint decision nor how to account for or link cases. Harmonising definitions and registrations seem an obvious means to achieve better transparency and comparability. Knowing how many complaints are being lodged, and what occurs to them, is crucial to assess and improve GDPR enforcement. There is no shortage of ideas from NGOs and academia about how to 'fix' the problem (European Digital Rights, 2022; Fuster et al., 2022; Masse, 2022; noyb, 2022).

As regards procedural changes, administrative law and a recent legislative proposal (Cooper et al., 2023; European Commission, 2023; Gentile & Lynskey, 2022) may address this issue. This is beyond the remit of this paper.

6.4.4 Practical KPIs to measure regulator effectiveness

Effectiveness and efficiency are often used interchangeably. They are different. As Peter Drucker (Drucker, 2016) put it: *"effectiveness is doing the right things, while efficiency is doing things right."* Effectiveness is about achieving strategic goals or outcomes. Efficiency is about achieving them with the minimum time, money or effort.

The regulators favoured hard metrics such as the number of complaints, investigations and fines because they are measurable and comparable from year to year (which is ironic since they are difficult to find and compare objectively by the public). The NGOs liked them because they were a tool for making comparisons and substantiating complaints against regulators they judged unresponsive. These are arguably as much a measure of efficiency as effectiveness.

Non-regulators favoured the softer metrics surrounding the public perception of improved control & understanding of rights and the business perception of clear guidance on compliant implementations. Regulators didn't like them because they were too subjective and regarded them as only having contextual significance. This may be missing the point. Article 1 of the GDPR states its objective is *"the protection of the fundamental right of natural persons and in particular their right to the protection of personal data."* The perception of stakeholders that privacy has improved and the regulation is implementable is a key desired outcome of the GDPR. Annual standardised sentiment or satisfaction surveys of both interest groups (and possibly NGOs) would reveal trends and inter-country differences without compromising the independence of regulators.

Enforcement in the form of large fines that deter and the media attention they attract were both seen as important and intertwined. Assessing whether a regulator is levying a proportionate fine amount could be related to the size of the country, industry, or non-compliant company turnover.

Assessing media impact is trickier. Different regulators carry different portfolios of responsibilities, which will impact the number of press releases they issue each year. Nevertheless, national regulators could easily identify in their annual report the number of GDPR-related press releases and the number of hits from it in the media.

Public perception could be measured by selectively borrowing marketing companies' techniques to measure brand value. For example, they use surveys and polls for quantitative analysis and focus groups and interviews for qualitative analysis. They use media analysis to monitor and analyze the coverage and sentiment of an organization in the media, and social media analysis to monitor and analyze the engagement and sentiment of an organization on social media platforms. All of these methods can help measure awareness, attitudes, opinions, satisfaction, behaviour, perceptions, motivations, emotions, experiences, likes, shares, comments, mentions, reviews, and ratings related to an organization. Obviously, the key challenge would be ensuring standardizing them for trans-European comparison purposes.

The budget KPI is an enabler. Regulators are not shy about complaining that they lack sufficient resources. A method to judge if their special pleading is justified would be to accompany their finances with comparable standardised benchmarks with other countries: the number of investigators, lawyers, and IT staff, for example.

The independence of a regulator from its government is a KPI that participants do not consider a priority at present. In the UK, there is a new data bill going through parliament. How far that will compromise its independence and imperil the UK's adequacy status is a subject of debate (J. Ryan, 2023).

Taken together, a standardised set of KPIs and standardised annual reports would significantly improve organisational learning, transparency, accountability, comparability and legitimacy of regulators.

6.4.5 Limitations & future work

Taking the methodology learnings from the previous two chapters, we decided to use a combination of semi-structured interviews and surveys. As before, these can come with generic response bias issues, although it was our experience that the regulators did not exhibit social desirability bias. They were straight shooters. The survey participants all came from the same stratum of management. The CISOs were all CISOs. Taken together, the relatively small number of interviewees and the skewed survey sample composition mean findings from this novel exploratory research come with standard caveats.

Most of the participants interviewed and surveyed were based in the UK, whereas the regulators were drawn from across Europe and did not include the UK regulator (who declined the invitation). The UK is no longer in the EU, but the EU deems its GDPR to have an equivalent adequacy status. The lead GDPR regulator, the Irish DPC, also declined to participate. Taken together, these three factors may affect the generalizability of the findings. In mitigation, while the business interviewees were heavily drawn from the UK (apart from one Irish company), all the regulators and NGOs had an international perspective, and most of the CISOs and executives worked in multinational companies with EU-based offices. Future work would benefit from a larger sample of interviewees and regulators Europe-wide. A logical next step would be to put numbers to the KPIs with the cooperation of the national regulators to enable in-country analysis and cross-country comparison.

6.5 Conclusion

Data protection regulations like the GDPR are increasingly important in securing individuals' privacy as society goes digital. The success of any regulation, however good, ultimately depends on how well it is executed. Existing literature fails to answer what good execution means in this context. We research what practitioners think are the objectives of data protection and privacy regulators and how they evaluate their effectiveness. We also explore novel methods for systematically assessing regulator performance in the future. Our findings indicate there is a gap between how practitioners judge regulators day to day and how they judge them when given a chance to discuss it in the round. The contrast between participants' initial criteria and their later ranking of the KPIs confirms this gap. Perception of the regulator's effectiveness is subjective, sanctions-focused and influenced by one's role and responsibilities. Regulators are designed to be independent of short-term political interference, but this raises serious questions of longer-term accountability. We examine the historical, cultural and organisational motivations behind the current byzantine complexity of the GDPR regime. Lastly, we contribute a series of key performance indicators and make structural suggestions around centralised and standardised reporting of cases to deliver improved learning, legitimacy, transparency and comparability. We believe our findings have important implications for the future development of regulator assessment and accountability in Europe and GDPR-like regimes outside Europe.

In the next Chapter 7, we take what we have learned about how the regulation and regulators' performance is currently assessed by practitioners in terms of the scope of citizens rights and data protection enforcement and reflect on how the impact of the GDPR may evolve in the near future in the face of changing circumstances. We will use scenario-based analysis to anticipate the context of the challenges it may encounter, understand their impacts and outline potential positionings of the GDPR.

Chapter 7

How might the GDPR evolve? A question of politics, pace and punishment

7.1 Introduction

The digital age has made personal data more valuable and less private. This is why privacy and data protection regulation is essential. The impact of the GDPR on global privacy regulation can be seen by the adoption of its principles and model by countries outside of Europe. The GDPR's pragmatic design, balancing the needs of various EU member states and translated into numerous languages, has fuelled its global influence. Whether it will continue to be a pacesetter and drive tighter privacy regulation or become a fig leaf for performative compliance remains to be seen. Our study explores future potential scenarios and how the GDPR might handle them.

It is important to bear in mind that scenarios as a scholarly methodology are not predictions (Ramirez et al., 2015). They are not meant to be 'right' or 'wrong', 'good' or 'bad', but to offer interesting, challenging, stretching or controversial future pictures. They provide a space—a sand pit—to challenge existing assumptions, identify novel lines of enquiry, and explore choices that various stakeholders might make under different market conditions.

We start with the premise that there is a global consensus that privacy in the digital world is worthy of protection, but approaches differ on the 'who' and 'how'. The US relies on market self-regulation, China trusts the state, and Europe employs arms-length regulators. As for the how, the enforcement strategies also differ, with the US favouring notice and consent while China and Europe adopt more prescriptive data protection regimes.

We analyse four macro drivers—econopolitical, legal, sociological and technological—shaping the regulatory landscape. Geopolitics and economic power will influence trade and shape cross-border data flow agreements. Robust enforcement is reliant not only on a legal framework but also on political will and

adequate regulator resourcing. Societal trust in technology companies, concerns about data security, and the influence of corporate lobbying will all weigh heavily on public opinion when debating the trade-offs between pro-innovation lighter regulation and pro-consumer protection frameworks. Advances in technology, for example in artificial intelligence (AI), will challenge the pace of regulatory adaptation.

Grounded in the driver analysis, we outline six thought-provoking scenarios out of 81 potential futures, each depicting the GDPR's accepted influence differently based on the drivers' interplay. Most versions envision a wider interpretation of existing principles or interaction with supporting regulations rather than changes to the GDPR's current legal text. Some scenarios see society accepting personal data sharing by default when using online services. Conversely, other scenarios redistribute power from Big Tech to citizens & regulators or the state bureaucracy, respectively, in a more human-centric model. Our analysis suggests the most likely outcome will be what we call Status Quo+ V1.2, a modest update to today's Status Quo V1.0, which raises questions about its adequacy in the face of technological advancements.

We argue the GDPR requires a more robust implementation, such as the Status Quo++ V1.5, to protect privacy. This entails stricter enforcement, countering the "regulation stifles innovation" narrative, greater cross-EU harmonisation, defending cross-border data rights, and proactive guidance from regulators on emerging technologies.

The paper is organised as follows: The contestable definition of privacy, the function of regulation, and the differing implementations of privacy regulation have already been covered in Background 2. With that as context, Section 7.2 constructs its analysis of the future in several stages, starting with structural forces and then condensing them into four key themes. Section 7.3 envisions six of 81 potential scenarios that shape six versions of the GDPR relative to GDPR V1.0. Section 7.4 discusses their plausibility and likely uptake. Section 7.5 concludes that while there is no silver bullet, the GDPR remains the best privacy armour we have today. By strengthening its effectiveness, we can ensure that the digital age empowers individuals, not just corporations and governments.

7.2 Analysis

For this research, we are forced to think about the future without hard empirical data. Instead, driver mapping and the political, economic, societal, technological, legislative and environmental (PESTLE) (Aguilar, 1967) analysis are used to identify forces that will shape the future policy environment. With the literature review as background, the analysis surfaces four themes that are the most salient for exploring future privacy regulation scenarios: (i) the geopolitical competition in extraterritorial jurisdiction, (ii) the robustness of enforcement, (iii) societal attitudes to the innovation versus risk narrative, and (iv) the challenge of keeping pace with rapid advances in the underlying technology. Of necessity, we maintain a euro-centric focus as this is a large canvas.

7.2.1 Method

Drivers and trends are vital components of future thinking. Drivers represent unquantifiable forces of change, like shifts in values and behaviours, acting as causes for developments. Trends are measurable, factual indicators of steady change, characterising developments. Combining trend and driver analysis forms a powerful tool for plausible scenario creation.

Scenario methodology as a scholarly form of inquiry is one way of generating interesting research (Ramirez et al., 2015). The scenarios are not predictions. Rather, they represent a multi-dimensional potential future space.

The PESTLE analysis framework (Aguilar, 1967) is applied to explore these dimensions systematically. It examines the Political, Economic, Social, Technological, Environmental, and Legal factors in the external environment. Invented over 50 years ago by American strategic planning scholar Francis Aguilar in his book "Scanning the Business Environment," (Aguilar, 1967) PESTLE is a strategic tool to analyse and monitor the macro-environmental factors that impact an organisation, company, or industry. It is widely used for horizon scanning (Boult, 2018) and to support evidence-based policy decision-making (Battista, 2024; Commission, 2018).

Political factors include government policies, trade regulations, and political stability. Economic factors include economic growth, inflation, employment, and globalisation impacts. Social factors include demographics, consumer behaviour, cultural trends, living standards. Technological factors include innovations, automation, and technology adoption rates. Environmental factors include climate change, environmental regulations, sustainability and energy consumption. Legal factors include health and safety regulations, intellectual property rights, consumer protection, and product standards.

To apply this framework, one identifies the relevant factors in each category for a specific market or organisation, gathers data, analyses their impact and prioritises the most significant factors. The analysis tends to be qualitative in practice. It is used to identify the signals of change and emerging trends that may have the greatest implications for a chosen policy area. The following sections will explore systematically each of the six PESTLE dimensions within the context of the GDPR environment and its stakeholders.

7.2.2 Geopolitical landscape

Geopolitics and data protection are tightly intertwined. In "Global Governance Challenges" (Carr & Llanos, 2021), Carr and Llanos describe three main approaches to governing data that currently coexist: a U.S. approach that treats individuals as data farms, a Chinese approach that governs through data, and an EU approach that tries to square the circle. The U.S. approach privileges the interests of its own commercial sector, where human rights and public goods are portrayed as protected by the private sector against misuse by the government. Online platforms have power to track, target and segment people into audiences highly susceptible to manipulation. It combines a poor data protection culture for individuals while ensuring online platforms are not subject to government surveillance. In the absence of overarching federal or state laws akin to the GDPR, US privacy regulation is increasingly being enforced by class action lawsuits albeit with mixed results. Refer to subsection 2.4.4 for more detail.

The Chinese approach follows the U.S. model regarding the widespread collection of personal data through consumer applications. There is a stronger narrative of utilising data for government purposes and for delivering a "public good." Data is used to calculate credit scores that integrate additional factors such as political activities and non-financial interactions. In a mirror image of the U.S., Chinese people have protections against commercial surveillance yet continue to experience relatively unconstrained government surveillance.

The EU approach attempts to stimulate innovation while protecting individual privacy in the data economy through the GDPR. It has meant individuals are bombarded by cookie notices, rendering consent devoid of meaning. And it has meant business is wary of experimenting with data, thereby threatening to cancel out its own goals. They conclude that the U.S. approach must change to maintain its dominance in the data economy to remain acceptable in democratic societies. The Chinese approach will appeal to some but impede strong ties with others. The EU approach may be the most advanced regarding democratic privacy protections for citizens, but how conducive it is to an innovative economy remains an open issue (Carr & Llanos, 2021)

The 'California effect' was formulated by Vogel (2009) and referred to nations adopting the higher, greener standards and regulations of the wealthier jurisdiction for trade-related purposes. He illustrated this with the case of California and its role in creating stricter automobile emission standards not only in the US but also abroad. The 'Brussels effect' (Bradford, 2020) was outlined by Anu Bradford and refers to how the EU is able to exert its regulations on other jurisdictions and influences antitrust, environment, health and privacy.

In "Digital Empires: The Fight to Regulate Technology" (Bradford, 2023), Anu Bradford paints a similar picture to Carr & Llanos, albeit arriving at slightly different conclusions. She, too, describes three digital empires and their models of regulating the digital economy, each organised around a different emphasis on the market, the state or the rights of digital citizens. She sees it in terms of horizontal and vertical axes: the horizontal axis is the battle between governments, and the vertical axis is the battle between governments and technology companies. In her analysis, the U.S. is losing the horizontal battle to China and the Europe Union. Authoritarian governments are turning to the Chinese regulatory model. Democratic governments are turning to the European regulatory model. Governments are not destined to lose their vertical battles against technology companies, albeit they are difficult to regulate. She sees it as a battle for the soul of the digital economy or a battle between techno-democracies and techno-autocracies.

Moving from this high-level perspective to a more data-level perspective, the traditional institutional framework underpinning regulations—around the sector or activity-focused ministries and agencies—shows its limits when dealing with the transversal challenges raised by the data economy. Data flows can span multiple regulatory regimes, creating the potential for confusion and risks. The on-off stalemate over the free flow of data between the U.S. and the EU best exemplifies this institutional and transboundary challenge. The latest deal, known as the EU-U.S. Data Privacy Framework (Fisk, 2023), was agreed in September 2023 after the Court of Justice of the EU (CJEU) struck down two previous agreements—known as Safe Harbour and Privacy Shield—after challenges by privacy activist Max Schrems. Both previous agreements were annulled over fears of snooping by U.S. intelligence agencies, exposed by Ed-

ward Snowden (Edward Snowden, 2015) and others. Schrems expects his latest complaint to come to the European Court of Justice in 2024.

The relationship between the GDPR and the Chinese PIPL is intriguing (Interesse, 2023). A pre-PIPL EU report concluded

> *"If a legalistic approach was adopted, then no common grounds could be found between two fundamentally different systems both in their wording and in their raison d'être. In addition, data transfers would need to be prohibited towards China, on the basis of Article 25 of the EU 1995 Data Protection Directive. However, this would be an impractical, if not unnecessary position."*
>
> (De Hert and Papakonstantinou, 2015)

As the Chinese economy has sputtered, China recently offered to reverse the burden of proof under their relevant laws, allowing most data stored in China to be transferred out of the country unless expressly excluded by the authorities (Politico, 2023).

The GDPR, CCPA and PIPL are all extraterritorial in their scope. The three data protection regimes apply to businesses worldwide that target their citizens, i.e., the GDPR applies to U.S. companies with EU customers. How the competing 'reach' of these laws affects cross-border data flow agreements will be a key factor in the future shape of the GDPR. Given that the U.S.-EU link is the most trafficked at present, we will consider a range of end-states: U.S. prevails, EU prevails, or both muddle along.

7.2.3 Legislative landscape

The success of a privacy regulation may be evaluated by identifying the desired outcome, such as discouraging non-compliance, encouraging good practice, or raising awareness of privacy rights, and comparing this to the result achieved. However, measuring compliance with privacy laws is more difficult than measuring enforcement. Thus we begin by examining the theory and track record of enforcement with regard to data protection regulations.

Before the GDPR took effect, the comparatively low maximum fines for corporate violations in prior data protection legislation led to a perceived lack of compliance by major U.S. technology companies. Fines were deemed "peanuts" or "pocket money" relative to the size of the companies (Fiveash, 2014; W. G. Voss & Bouthinon-Dumas, 2021). In theory, this has changed. Now EU Data Protection Authorities (DPA) can issue sanctions for data protection violations for up to the greater of €20 million or 4% of global turnover.

Sanctions reinforce legal imperatives by rewarding compliance or penalising disobedience. They can take the form of financial, administrative, or regulatory measures. Sanctions serve diverse purposes, including retribution, rehabilitation, expression of disapproval, and norm-setting. They can restrict liberty, impose fines, or compel specific actions. Symbolically, sanctions convey denunciation, aiming to correct past mistakes and deter future violations. Retribution, governed by the principles of effectiveness, proportionality, and dissuasion, requires a link between the fault or harm and the penalty's severity. Expressively, sanctions show society's commitment to values through procedures, fines, or actions. They also guide behaviour by detailing mandatory or prohibited actions. Although sanctions for data breaches may be symbolic and need not

be overly severe, the imperative remains for DPAs to diligently enforce regulations, preventing Big Tech from selectively seeking favourable jurisdictions (forum-shopping) (W. G. Voss & Bouthinon-Dumas, 2021).

However, through what is referred to as the one-stop-shop mechanism, the Irish DPA is the lead authority for most of the US Tech Giants, and critics claim it has failed to act against them up to now, resulting in a potential lack of deterrence (Nast, 2022; Wodinsky, 2022). While the Irish DPA has started to issue fines in the 100's of millions of euros more recently, it has only done so after allegedly much arm-twisting by other DPAs. The Irish are not unique. Differences in national laws, administrative processes and historical engagement with industry mean national DPAs come to the GDPR from different starting points. Differences in human and financial resources mean that DPAs have varying organisational capacities. And differences in political influences mean DPAs' self-confidence and understanding of their role may differ significantly between European countries. All these factors contribute to the noticeably different implementations and enforcement of the GDPR. Recent empirical research (Buckley et al., 2022) confirms intuitively that fines focus the minds of business leaders and are how the general public perceives the virility of their regulator (noyb, 2022; J. Ryan & Toner, 2020). Looking ahead to the next ten years, the degree to which the EU harmonises the motivation and capability of its enforcement function will be a key critical success factor. We will consider a spectrum of end-states ranging from the status quo, improved harmonisation to robust enforcement.

7.2.4 Sociological landscape

Big Tech companies have a complex and often adversarial stance towards regulation, generally favouring self-regulation over government intervention. They assert they are better placed than governments to regulate themselves as they have a deeper understanding of the technology and market landscape. They argue compliance costs associated with regulation will ultimately be passed on to consumers through increased prices (Cordes et al., 2022). Additionally, they express apprehension that regulation could hinder innovation, potentially delaying or preventing the introduction of novel products and services. Nick Clegg, President of global affairs at Facebook has warned EU legislation "risks fossilising ... experimentation that drives technological change". There is also a suspicion that the EU (Broadbent, 2020) want to hobble US technology companies to achieve European "tech sovereignty".

The pro-Big Tech argument is that it is arguably the most productive part of the US economy. The rate of innovation and spend on R&D is high. They are among the largest patent owners. They compete and there is little evidence of collusion. They pay their knowledge workers well. None of these are signs that they deserve opprobrium.

Historically, the data economy operated behind a "digital curtain," shielding its practices from public and legislative scrutiny, treating data as proprietary company assets despite its origin in customers' private behaviour. However, according to the Harvard Business Review (Rahnama & Pentland, 2022), a shift has occurred that is being driven by three forces. First, mounting consumer mistrust against "surveillance capitalism". Second, governmental interventions in the US, EU and China have challenged companies to comply across

diverse regulatory jurisdictions. Third, increased market competition, notably Apple's iPhone operating system upgrade enabling user control over data tracking, caused substantial financial losses for major social media platforms. Apple seeks to make privacy a market differentiator since it is arguably less dependent on the data economy than Alphabet or Meta. In response, Facebook and Amazon have agreed to share consumer data to compensate for losing access to the "walled gardens."

In the face of growing consumer dissatisfaction and several antitrust lawsuits in the US and fines in the EU, Big Tech has begun to signal a preference for comprehensive uniform regulation and support for industry involvement in policy development. Some observers question the industry's sincerity and wonder if their attitude to regulation is not akin to the famous prayer attributed to Saint Augustine "Oh God, make me good—but just not yet" (University, 2024). This tension between the innovation narrative, profit motives, and the societal impact of these technologies remains another central driver in the future shape of the GDPR. Against this backdrop, we will consider three end-points: pro-innovation prevails, ex-ante prevails or a bit of both.

7.2.5 Technological landscape

Here we look at the intersection of law and technology and how the sheer speed of technological change fundamentally challenges contemporary regulation. Digital technologies tend to develop faster than the regulations or social structures governing them. While this disconnect has always been a concern, there is mounting press attention about how GDPR is failing to keep pace with potential privacy-invasive technologies.

The bones of the GDPR were agreed upon by Members of the European Parliament (MEP) as far back as 2012, adopted in 2016, and came into force in 2018. In some senses, the GDPR is already ten years old. New technologies such as blockchain and Artificial Intelligence (AI) have emerged in the meantime (European Parliament. Directorate General for Parliamentary Research Services., 2019). Multiple tensions exist between blockchain and the GDPR such as who is the responsible or accountable data controller in a decentralised system and how can data be modified or erased in a system designed to resist unilateral changes to ensure data integrity and trust. Another example of the tension relates to data minimisation and purpose limitation. Blockchain is an append-only database. Old data cannot easily be moved and its purpose is questionable under GDPR since the initial transaction is retained as part of the continuing consensus usage. Similar tensions and proximities exist between AI and data protection principles, such as purpose limitation and data minimisation. A recent EP study (European Parliament. Directorate General for Parliamentary Research Services., 2020) concludes that AI can be deployed in a way consistent with the GDPR, but also that the GDPR does not provide sufficient guidance for controllers and that its prescriptions need to be expanded and specified.

The goal of GDPR is to protect personal data against unnecessary collection. However big data and IoT combined with machine learning and AI means it will not be difficult in the near future to re-identify individuals by cross-triangulating data. The personal data/non-personal data distinction will become untenable. In 2008, the film rating records of 500,000 Netflix subscribers were re-identified using the public Internet Movie Database (Narayanan & Shmatikov, 2007).

More recently in 2019, researchers published a method to correctly re-identify 99.98% of individuals in anonymised datasets with just 15 demographic attributes (Rocher et al., 2019).

Some critics (Tene & Polonetsky, 2012) argue that the binary labelling of information as either 'personally identifiable' or not, is meaningless in a Big Data age. They view the identifiability of data as a continuum as opposed to the current dichotomy. Some go further and argue that GDPR risks becoming the regulation for all data and not just personal data and, therefore, unworkable since the majority of the data universe relates to people and their interactions with connected technology that throw off data as normal. Other academics, such as Jaap-Henk Hoepman, reject this fatalism. He argues in "Privacy is Hard and Seven Other Myths" (Hoepman, 2021), that just as technology can be used to invade our privacy, it can be used to protect it when we apply privacy by design (PbD) from the outset.

Thus, how regulation keeps pace with new technology or how regulatory technology (Wikipedia, 2024a) (commonly abbreviated as RegTech) takes advantage of it will be critical to the future success of the GDPR. At one extreme, people fear that AI's data collection, online monitoring and predictive profiling capabilities will be able to anticipate individuals' future actions and opinions (a la the pre-cogs in Hollywood's Minority Report or the restaurant that knows what you will select before you see the menu in an episode of Black Mirror) and thereby make privacy and GDPR an irrelevance. In this scenario, the bad actors could either be state actors, Big Tech or organised crime using rogue AI to circumvent RegTech. At the other extreme, people can imagine AI as a personal privacy guardian and AI-driven RegTech being used to audit algorithms and training data in collaboration with other regulatory bodies globally. In between, one can imagine a messy patchwork of algorithm transparency and accountability in some regions, loopholes in others, where GDPR's vaguer principles come into play and set the scene for a protracted series of test cases where regulators race to update the guidance of a largely unchanged GDPR. Thus we will consider a spectrum of end-states: GDPR becomes unfit for purpose, GDPR is AI-enabled and GDPR guidance is firmed up over time.

7.2.6 Summary

Combining the background briefing on regulation theory & practice in the literature review section and the driver and trend analysis in this section, the resultant synthesis surfaces four themes, each with a spectrum of potential end-states, that are most salient for exploring future potential privacy regulation environments. In summary, the first theme is the geopolitical battle for global influence that manifests itself most clearly at the interface of cross-border data flow agreements and the clash of extraterritoriality. The second is the struggle by EU regulators to coordinate and enforce fines against well-funded corporates. The third is the ongoing debate between pro-business, low-regulation advocates and pro-consumer, high-regulation privacy champions. The fourth is the evergreen challenge of keeping up with fast-moving technology. These four themes are not independent. Their interactions can act as positive or negative feedback loops. For example, rising pro-consumer sentiment would likely result in increased funding for regulators and more proactive enforcement. Conversely, pro-business sentiment would likely result in lower funding for regulators and

less intrusive regulation. We assume the political backdrop will likely remain stable over the next decade: a laissez-faire US, an autocratic China, and a rights-based EU.

7.3 Results

As summarised in Section 7.2.6, the output is a fictitious futures space bounded by four themes, each with a spectrum of possible end-states. The resultant combinations allow us to explore different pathways and outcomes. Given there are $3 \times 3 \times 3 \times 3 = 3^4 = 81$ possible combinations, we use abductive reasoning which is a form of logical inference that seeks the simplest and most likely conclusion from a set of observations to narrow down the universe of potential scenarios.

7.3.1 Rationale

We start with the current geopolitical situation and frame the present GDPR as version 1.0 or V1.0. The scenarios will be labelled with version numbers relative to V1.0 and visualised in Figure 7.1, to show their relative positioning and summarised in Table 7.1 at the end of this section. While geopolitics and economics do not invariably trump local politics, it is reasonable to assert that they will play a pivotal role in an increasingly global digital data economy. If this driver and power dynamic remains unchanged, we anticipate minimal shifts across the other themes, and changes to the operation of the GDPR would be modest and procedural rather than substantive: let us call it the status quo+ or V1.2 to reflect its positioning relative to V1.0. If the geopolitical and economic landscape tilts more in favour of the US, then it is improbable there will be substantial change to the GDPR across the other themes. In fact, personal data protection may deteriorate slightly compared to today: let us call it V0.8.

Now let us consider what would happen if global affairs were inclined more in favour of the EU. A new self-confidence could lead to better-coordinated enforcement and a reevaluation of innovation-v-protection priorities: let us call it the status quo++ GDPR or V1.5. Should the global attitude towards data protection (at least in Western democracies) align firmly in with European principles, then we could see a much stronger GDPR, which we will call Europe GDPR or V2.0. A variant worth exploring would be what would happen if European data protection values were adopted widely but Europe started to copy Chinese practices: let us call it Centralised GDPR or C2.0. Finally, the wildcard driver is technology. What if technological development accelerated beyond our control and our laws? We dub this the AI GDPR or version 0.0 to reflect that it might undermine the GDPR, if only temporarily.

Table 7.1 summarises the six scenarios in a version-dimension matrix.

An alternative way to picture this narrative is to imagine a space defined by a citizen's rights axis and a data protection enforcement axis as visualised in Figure 7.1. Versions V1.2, V1.5 and V2.0 represent implementations with progressively stronger privacy rights and enforcement mechanisms, whereas V0.8 is the more diluted alternative to the current V1.0. The AI V0.0 version epitomises an uncertain regulation struggling to find its relevance in a chaotic, innovation-friendly environment. The C2.0 version is the centralised, dirigiste twin to V2.0

Table 7.1: Scenario Matrix

Scenario	Geopolitical	Legal	Societal	Technological
V0.0	Confused	Low enforcement	Uncertain	AI-driven irrelevance
V0.8	Pro-US	Patchy	Pro-innovation	Slow obsolescence
V1.2	Status quo	Improved	Status quo	Slight scope upgrade
V1.5	Tilt to EU	Coordinated	Tilt to pro-consumer	Wider scope application
V2.0	Pro-EU	Stricter	Pro-consumer	Self-regulating PbD
C2.0	Centralised EU	Strictest	Pro-consumer	Strategic EU control

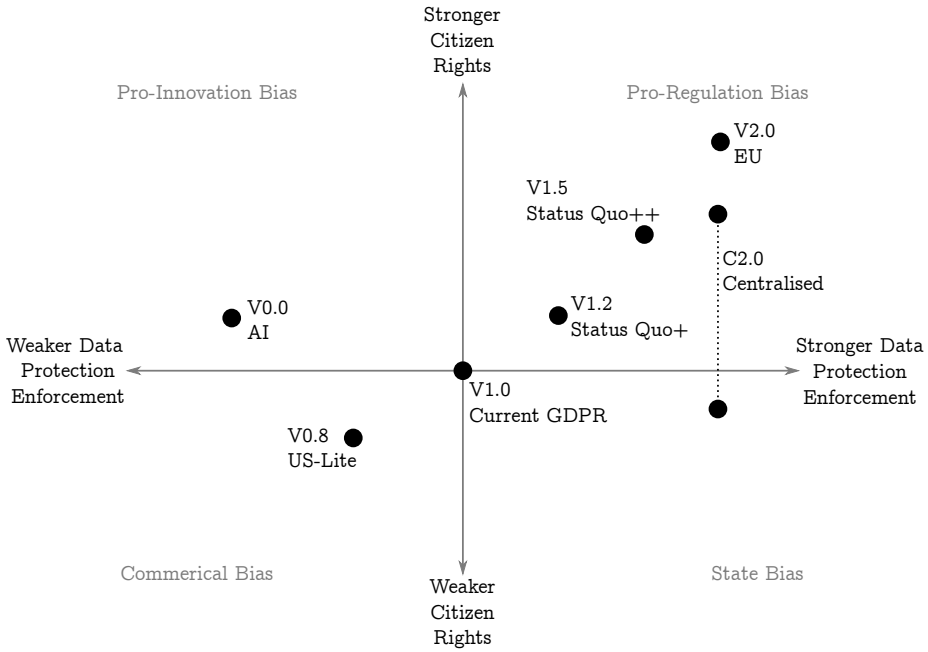


Figure 7.1: Version Positioning

but with the important caveat that it may compromise citizens' rights if it conflicts with the interests of preordained regional champions. To round it off (but not included to avoid over-complicating the picture), the current Chinese and US data protection regimes can be imagined sitting in the lower half of the figure.

Remember, the six scenarios are not predictions. They are not meant to be 'right' or 'wrong', 'good' or 'bad', but to offer interesting, challenging, stretching or controversial future pictures. They provide a sand pit to challenge existing assumptions, identify novel lines of enquiry, and explore choices various stakeholders might make under different market conditions.

Also bear in mind that the versions are not necessarily new regulations per se. Some reflect different emphases of implementation rather than new legal text since the GDPR already contains many principles ripe for revised interpretation. Moreover, they will interact with newly emerging EU regulations in adjacent spaces (as outlined in Section 3.3). For example, a 2020 report for the EP concluded that AI can be deployed in a way that is consistent with the GDPR, but also that the GDPR does not provide sufficient guidance for

controllers, and that its prescriptions need to be expanded and concretised (European Parliament. Directorate General for Parliamentary Research Services., 2020).

Next, we describe and critique the scenarios in more detail.

7.3.2 AI V0.0

This is the nightmare technology-driven scenario. Contrary to the optimistic 2020 AI Impact EP report (European Parliament. Directorate General for Parliamentary Research Services., 2020), the GDPR is discredited and widely regarded as unfit for purpose. AI creates new privacy risks like deepfakes and physiognomy or exacerbates existing privacy risks. Mass surveillance and minute quantification of individuals' lives become possible. As imagined in sci-fi literature, privacy is not personal—privacy is theft (Eggers, 2013). Surveillance, data and shame become socially accepted behaviour modifiers (Eggers, 2021). Commercially, it assumes the pro-innovation narrative prevails, which blocks preemptive legislation. Untrammelled accelerating development of AI runs rings around concepts such as informed consent or data minimisation. Geopolitically, the US, EU and other Western democracies muddle along while the internet splinters into protectionist sub-domains by more autocratic regimes. Lacking a global consensus, enforcement becomes nigh impossible without an agreed legal framework. The GDPR and similar legislation remain 'on the books' while policymakers struggle to augment it or replace it with a new AI-ready version. In effect, it is obsolete.

This GDPR fails to keep pace with technology and is different to all the other versions. It assumes the GDPR will have to be replaced or dramatically amended. All the other versions of GDPR imagine minor amendments or stricter implementation of the existing GDPR. This scenario posits there will be an interregnum where regulators lose track of what AI can do and is doing with personal data. Algorithmic transparency and enforcement become moot. Formulating a new regulation to replace or materially extend the GDPR would be a herculean task involving a formal proposal, legislative negotiations with the European Parliament (EP) and the Council of the European Union, and stakeholder consultations. In the end, however, one assumes common sense prevails, and a new post-AI privacy norm becomes codified.

Some scholars (Parikh, 2024) warn that AI may grow faster than expected due to its pervasive effects on the economy, its ability to improve rapidly and how it may spawn complementary innovations. The investment markets' enthusiasm is tempered, however, by the significant capital expenditure required to develop cutting-edge AI products and to defend mounting copyright challenges. The water and energy required by AI data centres are already encountering pushback in a number of host countries (Yale School of the Environment, 2024). A market analyst (Hodgson & Kinder, 2024) characterised Alphabet and Microsoft customers as being in "buy AI now, figure it out if it works later mode". Time will tell if AI is the next tulip bubble or a revolutionary innovation.

7.3.3 US V0.8

This is the Americanised GDPR against a backdrop of slower advancements in technology. Geopolitically, it assumes the EU has to relent on cross-border data

flows and agree to US demands. Enforcement against Big Tech continues to be fragmented and underpowered. Enforcement in specific sectors like insurance continues to rely on class action lawsuits for privacy violations. The mantra "move fast and break things" reigns supreme. The success of the pro-innovation narrative undermines support for regulation. This, in turn, means the GDPR is blocked from keeping pace with new technologies such as AI or biometrics. The GDPR is frozen in time. As time marches on, it becomes less relevant and backslides. Hence, it is referred to as V0.8 relative to V1.0 today.

If Max Schrems successfully challenges the latest transatlantic agreement regarding data flows between the US and the EU, it could have significant implications for the GDPR. The EU-US Privacy Shield, the predecessor of the recent agreement, was previously invalidated by the European Court of Justice (ECJ) in the "Schrems II" case, where Max Schrems argued that US surveillance practices did not meet EU privacy standards (CJEU, 2020). If the new agreement is invalidated, it could trigger EU authorities to reassess and potentially weaken or strengthen mechanisms for cross-border data transfers. In other words, this scenario could be the genesis of the US-friendly version or the V1.5 update to the GDPR.

In the US-friendly scenario, the EU accepts it will never persuade the US to relax its national security powers under the Foreign Intelligence Surveillance Act (FISA) (US Department of Justice, n.d.) to the extent that it would satisfy the GDPR. While US politics is not as great a believer in collective action as Europe, national security is one of the rare exceptions. Given the commercial downsides are clear for businesses relying on transatlantic data transfers, the EU would have to relent and instead focus its energies solely in Europe. US companies would still be subject to the GDPR in the EU but not as constrained outside the EU. As a foretaste of things to come, we saw the curious manoeuvre in 2020 when Google announced it was transferring data about UK users of its services to US jurisdiction to avoid GDPR complications post-Brexit (Murgia, 2020; Tuta, 2020). In the end, the UK GDPR was deemed 'adequate' by the EC and continues to be able to transfer data to other countries covered by an adequacy decision.

7.3.4 Status Quo+ V1.2

This is an incremental improvement on today. It is the status quo+ GDPR. It assumes the EU and the US compromise on cross-border data flows to neither party's satisfaction. The one-stop-shop mechanism undergoes limited harmonisation, resulting in slightly better cross-border enforcement. There is gradual scope creep in applying the GDPR to new technologies. Still, progress is slow in the face of the anti-innovation narrative, industry lobbying and constant challenges in court. V1.2 is more effective than version 1.0, but not by much.

The status quo version of the GDPR takes account of the in-built inertia. It assumes there will be modest improvements in EDPB guidance and enforcement harmonisation. It has the advantage of maintaining the known current data protection regime while keeping its powder dry for future developments. Companies know where they stand and how to comply, while critics like Noyb complain that authorities fail to get businesses to comply properly.

7.3.5 Status Quo ++ V1.5

This is a material advance on today. It is the next-generation GDPR. It assumes the US compromises on cross-border data flows and agrees to stronger protections for non-US citizens. There is material harmonisation in the one-stop-shop mechanism, resulting in stricter enforcement. The pro-consumer narrative wins, provoking increasing demands for more consumer rights and transparency, which translates into wider application of the GDPR to new technologies. V1.5 is still recognisably the status quo but with significant adjustments.

In this scenario, the EU sticks to its guns. It presses ahead with known areas that require improvements, particularly with regard to more robust and coordinated enforcement. It could be argued that Big Tech might benefit in the long run if their incentives were more in alignment with the GDPR. Recent scandals, rising fines and diminishing customer trust compromises the growth of the digital ecosystem in which they thrive. Microsoft is a case in point. It was a company of immense power and had no incentive to change until it came under political pressure and anti-trust investigations after being accused of stifling competition in the browser market. It had to change and adopt new practices. This allowed Google to emerge and enrich the entire digital ecosystem. Microsoft is still very successful. It is one of the few Big tech companies not under constant severe scrutiny by regulators nowadays.

A stronger implementation of the GDPR may also inadvertently benefit Big Tech in other ways. Early empirical analysis by Koski and Valmiri (Koski & Valmari, 2020) has shown that European data-intensive SMEs were the most disadvantaged group regarding their post-GDPR profit developments, while the large European data-intensive companies' short-term post-GDPR profit margins dropped relatively less. Compliance overheads may be proportionately higher for SME's (Buckley et al., 2024b) and they may face stricter enforcement as there is a perception that regulators find it easier to handle smaller organisations than big multinationals (Manancourt, 2021). In the keynote speech at the recent European Data Protection Summit conference in June 2024, Viviane Reding (former Vice President of the European Commission 2010-2014 and one of the key architects of the GDPR), put it in a forthright manner. She said she wrote the GDPR to protect us from Big Tech & Government - not the village butcher & football team. Unfortunately, "national regulators looked more for the nitty gritty than for the real problems with the big platforms" (Reding, 2024).

7.3.6 Europe V2.0

This is the maximalist version. It is the pro-privacy GDPR. The assumed US climbdown means the GDPR becomes the global standard on cross-border data flows for most of the world. The application of the principles is expanded to cover more uses and technologies. Strict harmonisation of the one-stop-shop mechanism and stricter enforcement means companies begin to embrace the philosophy of Privacy by Design (PbD) and self-police themselves to avoid the potential of crippling fines. V2.0 vision is closest to what digital rights activists such as noyb (noyb, 2024) would see as necessary to protect privacy.

At first glance, the maximalist GDPR may appear to be the polar opposite, but it is not that far removed from the Chinese GDPR. Europe looks at China's success but draws different conclusions. It, too, introduces stronger rights and

controls over personal data, reinforcing the principle of user autonomy and consent and raising the overall standard of privacy protection for EU citizens. It imposes more stringent reporting obligations on businesses, fostering a culture of corporate accountability and responsibility. It introduces more severe penalties for non-compliance, serving as a strong deterrent against data breaches and misuse of personal information. All of this combines to build consumer trust in the European digital ecosystem. Unlike China, which prioritises the interests of the state and party over individual privacy, this version seeks to impose restrictions on both commercial entities and government bodies.

Far from stifling innovation, it reinvigorates it. Companies compete to build better privacy-by-design platforms. GDPR portability provisions, for example, mitigate platform lock-in and spawn a new generation of integrative competitors to the incumbents. If privacy is really the new market differentiator, Europe has the opportunity to be the leader, unlike some US companies that talk the talk but may not be regarded as sincere in the quest to prioritise societal privacy. A maximalist GDPR instils confidence in global partners and facilitates cross-border data flows and commerce.

The downside of the maximalist GDPR may be that it indeed stifles European innovation further and US technology companies either exit the market (as Google did in China) or design truncated versions of their services to satisfy the regulations (as many companies have done to remain in China). Such strict measures, seen in some quarters as protectionist, would encourage domestic replacements but leave European citizens with potentially less than best-in-class substitutes.

7.3.7 Centralised C2.0

This is the GDPR where the EU adopts a style of regulation similar to China. It assumes there is a robust defence of EU cross-border data flows. Sanctions for violations are strictly enforced. The application of the regulation is at the discretion of the regulators and not as predictable or transparent as before. Seats on the boards of large technology companies, classified as strategic players, are reserved for EU technocrats. The EU is still a rights-based organisation, avoiding any surveillance state comparisons with China, but defiantly protecting and promoting its commercial interests.

The Chinese-style GDPR may seem far-fetched, but it may be quite pragmatic. According to Oscar Wilde, “imitation is the sincerest form of flattery”. If so, China has already shown it is not above learning from and copying many aspects of the GDPR in its own regulation. So why shouldn’t Europe? After all, the Chinese economy continues to grow faster than Europe. It continues to breed national champions in technology unlike Europe. It has pioneered dual-use technology that has civilian and military applications and amplifies its potential export markets. Critics may shrink from facial recognition and other state surveillance applications, but there are ample examples in the West already where governments are studying usage for crowd control, law enforcement and state benefit fraud, and corporations use software to surveil work-from-home (WFH) employees. China has off-the-shelf solutions because it has encouraged technological innovation while enforcing robust privacy regulations. It has required its platform companies, for example, to take more responsibility for resourcing and building the tools to identify and restrict the spread of mis-

information. The state places its representatives on the boards of its Big Tech to keep them aligned with state and societal priorities. In ten years' time, who is to say that Europe will not be looking over its shoulder and adopting similar strategies? One can imagine a 'Europe First' movement could emerge, mirroring the 'America First' approach seen in the United States. This might lead to European technology companies receiving favourable treatment in government contracts for strategic sectors. Interestingly, a more dirigiste or interventionist EU might occasionally find its goals at odds with its citizens' rights, explaining why C2.0 is depicted as a range in Figure 7.1.

The flip side of the Chinese model is that there is evidence that over-tight control may already be restricting strategic freedom at the boardroom level (Hijmans, 2018) and chilling innovation in AI over content restrictions (Q. Liu, 2023). Furthermore, some countries may be put off being identified with Chinese-style state control.

7.4 Discussion

Data privacy is as relevant now as when the GDPR was drafted almost a decade ago. Digital privacy concerns have not diminished in the interim. In fact, recent developments in technology like AI that postdate the GDPR confirm our scenario analysis that the GDPR will require additional impetus, guidance, and possibly regulation to address existing and new challenges to privacy.

Our scenarios are not predictions. They are not 'right' or 'wrong', 'good' or 'bad'. They offer stretching future pictures. They challenge assumptions, identify novel lines of enquiry, and explore choices stakeholders might make under different market conditions. And they can never be exhaustive.

When we consider our four drivers, there appears to be a clear hierarchy. Changes in geopolitical and economic conditions have the potential to cause the most change. Extreme political upheavals like a revolution in communist China, a civil war between red and blue states in the US, or a breakup of the EU would undoubtedly be transformative in unpredictable ways. Less extreme political changes, like a change in the US or Chinese presidency or a shift to the right in Europe, still have the potential to reframe the situation radically. For our analysis, we have eschewed these extreme scenarios. Still, even an economic depression or trade war might encourage populist politicians to unshackle business from pesky regulations and thus enforcement of them. Apart from a few recent multi-million euro fines by the Irish DPC, a persistent criticism of GDPR regulators is their reluctance to enforce large fines in contrast with financial regulators. New technology or advances in privacy-enhancing technology could make privacy regulations irrelevant. The link between societal concerns about privacy and the demand for tighter regulation seems the weakest driver. The Snowden revelations (Edward Snowden, 2015) are known to have helped push the GDPR across the line in the European Parliament. On the other hand, subsequent revelations about surveillance capitalism and spyware for sale, such as NSO's Pegasus (Wikipedia, 2024c), have not had a similar impact. This failure to capitalise on societal concerns in the public forum may be explained by the traditional aloofness of regulators as well as the undoubted imbalance between well-financed corporate lobbyists on the one hand and digital rights campaigners and consumer groups on the other.

There are reasons to be positive about the prospects for the GDPR over and above those already discussed. The EU has set the regulatory pace even where its domestic data technology industries are undersized because it is prepared to think and act systematically where other jurisdictions have not. In fact, the absence of a strong domestic industry has possibly helped rather than hindered the EU's leadership and impartiality on data protection. There is a strong incentive for the EU's trading partners to implement interoperability, if not full harmonisation since multinationals want to transfer personal data across borders. Large companies can ill afford several data centres that abide by different regulations. Backend systems are costs that are there to be culled. The GDPR is an anchoring or triangulation point to which other countries can refer for inspiration (if not quite a copy-and-paste template) when creating their regulation.

That said, the GDPR faces headwinds at home and abroad. For example, no sooner had the EU and MEPS in the European Parliament agreed to a draft AI Act in December 2023 than President Macron criticised it for excessive regulatory zeal. Observers suggested this reaction may have been driven by a protectionist impulse to protect a rising domestic star in AI. The scope for internal rivalries between member states to scupper well-motivated initiatives should not be underestimated, nor the scope for non-EU states to offer more libertarian and less costly regulations that undercut the GDPR. Cédric O (Prescott, 2024), a former French minister for technology, wrote on Twitter/X that through these laws, the EU was carrying the can for US businesses: "One would expect the United States to take some responsibility for the consequences of the shortcomings of their digital actors, who incidentally wield considerable global influence. Yet, there is (almost) nothing. Europe is left to carry the burden, often at the expense of its own competitiveness."

The new AI Act is another complicating factor. It is still too early to say what impact it will have on the enforcement of the GDPR. As such, the AI Act is out of the scope of this article, but it will make for an interesting analysis for future work.

All six scenarios are possible. The Centralised C2.0 and the maximalist Europe V2.0 are the least plausible. While there will continue to be a push to toughen up privacy regulations to V2.0, it will be tempered by industry lobbying and fear that it might stifle innovation and put the EU at a competitive disadvantage. For example, "In AI, Europe should innovate before it regulates," Macron's Finance Minister Bruno Le Maire said last year ahead of the AI Safety Summit in the United Kingdom, continuing "Regulation is indispensable, but it will be more effective if we have European players mastering AI" (Volpicelli, 2024).

The same forces would be at play doubly against the Centralised C2.0. Any suggestion that the EU should reserve board seats for its technocrats would face dramatic organisational evasive tactics by multinationals, jockeying for plum roles by EU technocrats and worries by liberal democrats that the EU was becoming too authoritarian.

V0.0 seems far-fetched. Society has become sensitised to the risks to privacy from emerging technologies such as AI. Already, there is public disquiet surrounding the mass consumption of data for AI training and the EU has put the industry on notice by announcing harsher than GDPR risk-tiered penalties of up to 7% of global turnover for non-compliance in the new AI Act. That

said, no regulation can anticipate all unintended eventualities or consequences.

The US-friendly V0.8 and the mid-range GDPR V1.5 seem more probable. V0.8 merely accepts the EU has a weak hand commercially and has to relax its resistance to the US FISA Act. The other side of the coin, V1.5, assumes a mix of consumer disquiet in the US and dogged protectionism of human rights in the EU, which compels the US to revise the FISA Act and relax its surveillance powers. V1.5 appears to be the bare minimum required to keep pace with inevitable technological advancements.

V1.2 seems most likely. It acknowledges minor tweaks to the GDPR in the pipeline but nothing else. It relies on institutional momentum to deliver agreed improvements. It also relies on the bunching or ganging-up effect of complementary legislation to strengthen its effectiveness. V1.2 will please business but may not be in society's best interests for all the reasons discussed heretofore.

7.5 Conclusion

There exists a global consensus that digital privacy deserves protection, but approaches differ. The US favours market self-regulation, China entrusts the state, and Europe utilizes independent regulators. The US model relies on notice and consent with light federal oversight, while China and Europe enforce prescriptive data protection regulations.

The EU's GDPR is widely regarded as the leading privacy regulation globally, evidenced by countries outside Europe adopting its principles. This study explores potential future scenarios and how the GDPR might evolve to handle them.

Scenarios as a scholarly methodology are not predictions. They paint plausible future pictures that challenge assumptions and stimulate new lines of inquiry.

Four key drivers could disrupt the status quo: geopolitics, enforcement capabilities, public opinion, and technological change. Geopolitically, major trading blocs export their privacy models based on relative economic and political clout, with the stronger dictating cross-border data flow terms. The ability to legislate and allocate enforcement resources impacts regulatory strength. Societal trust in technology firms' data practices shapes public demand for more or less regulation. Rapidly advancing technologies, especially AI, pressure regulators to update rules quickly.

Analysing these drivers, we outline six thought-provoking scenarios out of 81 potential futures, each depicting the GDPR's accepted influence differently based on the drivers' interplay. Most versions envision a wider interpretation of existing principles or interaction with supporting regulations rather than changes to the GDPR's current legal text. The AI V0.0 and US V0.8 scenarios see society accepting personal data sharing by default when using online services. Conversely, the V2.0 and C2.0 scenarios redistribute power from Big Tech to citizens & regulators or the state bureaucracy, respectively, in a more human-centric model. Our analysis suggests GDPR's most likely path is Status Quo+ V1.2, a modest update insufficient for addressing technological advancements.

We argue the GDPR requires a more robust implementation, such as the Status Quo++ V1.5, to protect privacy. This entails stricter enforcement, countering the "regulation stifles innovation" narrative, greater cross-EU harmonisation, defending cross-border data rights, and proactive guidance from regulators

on emerging technologies. While imperfect, GDPR remains the strongest privacy armour today. Strengthening its effectiveness can ensure the digital age empowers individuals, not just corporations and governments.

Chapter 8

General discussion and conclusion

The central research question is how do we, as a society, take back control of our personal data. In the mid-90's, I was Director of Marketing & Information Technology for Europe's largest commercial credit rating agency. At the time, I was astonished by how much information we collected on companies by taking data feeds from utilities, Companies House and media sources. A decade later, I led a fraud detection platform that leveraged mobile phone data to identify organised crime rings. Again, I was amazed by how combining static and dynamic data could reveal so much about the activities of criminals. However, it was not until I commenced my Masters Degree in Information Security in 2018 that I truly grasped the unprecedented scale of Facebook and Google's data collection capabilities, which far exceeded my imagination. For my MSc dissertation, I studied data trusts, a combination of systems and legal structures that attempted to manage individuals' data on their behalf and thereby wrest back control. I discovered they showed potential but their long-term effectiveness was unproven. I considered technological solutions but even the ICO cautions " You should not regard PETs as a silver bullet to meet all of your data protection requirements" (ICO, 2024). Its reservations are spelt out more boldly in other papers like 'Why PETs may not be our best friends' (Renieris, 2021), which argued that PETs were complex, expensive and resource-intensive, hard to implement and prone to user error. It asserted that PETs could create a false sense of safety and security. As a result, PETs may perpetuate the status quo and prevent reforms or changes to business-as-usual by reducing the urgency to act. Gradually, I became interested in studying the politics, philosophy, and economics of privacy and security and, later, the structural role of law in countering rampant surveillance capitalism. Since the GDPR is the most recent and comprehensive regulation to address data privacy concerns, it presented a compelling opportunity to study its contribution to the central research question and derive insights that could inform new privacy-related regulations. This PhD thesis concludes that while the GDPR has been effective in partially redressing the power imbalance between individuals, data-driven businesses, and governments, it should be viewed as a work in progress that requires continuous assessment and refinement.

In this chapter, I provide a (i) Summary of the key findings, (ii) Interpretation of results, (iii) Limitations of the study, (iv) Implications and contributions, (v) Future research directions, and (vi) Concluding remarks.

8.1 Summary of research

Chapter 4 describes how regulation is a vital government policy lever for better economic, environmental, and societal outcomes. The EU's GDPR exemplifies this in data privacy and security. While attention has focused on GDPR's benefits for regulators (stronger powers) and consumers (stronger privacy rights), I explore potential business benefits and how they affect different organizational components since it is business that incurs the cost of compliance. Prior literature proposed potential GDPR business benefits like better data management/analytics, brand enhancement, and a level playing field, but empirical follow-up has been lacking. Through semi-structured interviews, I investigate the perceived benefits of GDPR to business and where its effects are felt within the organisation. I find the threat of large fines has made businesses more privacy-conscious. GDPR provided justification to invest in modernizing data management and security processes. Companies now have cleaner, more up-to-date customer databases. Without GDPR, they admit to overzealously collecting, overusing, retaining, and undersecuring data. GDPR created new organizational power bases acting as privacy champions, whose influence hinges on regulators maintaining enforcement/breach visibility.

Chapter 5 analyzes the unique dual perspective of individuals who have implemented GDPR at work while also benefiting from it as consumers. Unlike prior studies focused solely on consumers or data professionals, this is the first empirical research into how these informed individuals perceive the cost-benefit tradeoff of their consumer privacy rights versus the pressures GDPR places on employers to support those rights. With the benefit of hindsight, I investigate if they think GDPR has been worth it. Through a multi-stage survey of individuals working at the same companies before, during, and after GDPR implementation, I study six hypotheses: Consumer awareness and knowledge of the GDPR and the regulator: Consumer feelings about privacy since GDPR was introduced: Observed company changes in response to GDPR: Employee awareness of the regulator in a work context: Observed benefits to their company from implementing GDPR. The survey finds participants recognize their rights when prompted but know little about the regulator. They have observed concrete workplace data practice changes and appreciate the tradeoffs. They're comforted that personal data is handled as carefully as client data. Surprisingly, those executing GDPR consider it positive for their company and privacy, contradicting conventional anti-regulation narratives.

Chapter 6 shifts the focus to the regulators overseeing and enforcing the GDPR. Any regulation's success ultimately depends on how well it is executed, but existing literature fails to define good execution in a data protection context. Measuring regulator performance is generally difficult since it is the regulated, not the regulator, who delivers the desired outcome. Many external factors are beyond regulators' control and can impact long-term outcomes. Assessing a GDPR regulator's performance adds more complexity, given privacy's contestable nature and differences in regulator make-up from country to country.

This complexity explains why the research is scarce.

I survey CISOs and conduct structured interviews with informed executives, lawyers, digital rights activists, and four national regulators, supplemented by enforcement database analysis. I investigate how the effectiveness of the GDPR regulator is judged and how we could better measure their performance. I find a mismatch between the broad presumed objectives attributed to regulators and the narrow sanction-focused criteria used to judge them in practice. Perception of effectiveness is subjective and influenced by one's role/responsibilities. Moreover, the intentional independence insulating regulators from politics raises accountability questions. I contribute key performance indicators and suggest centralized, standardized case reporting for improved learning, legitimacy, transparency, and comparability.

Chapter 7 is a playful thought piece about the future of the GDPR in the next decade. The GDPR's pragmatic design, balancing the diverse interests of EU member states, and translated carefully into world languages, has fueled its global influence and adoption. Given its importance, I explore where the GDPR may evolve in response to changing conditions over the next decade. I analyze the U.S. (self-regulation), Chinese (state control), and European (arms-length regulator) approaches through a PESTLE (political, economic, sociological, technological, environmental, legal) framework, identifying four key drivers shaping the future regulatory landscape: geopolitics, enforcement capacity, societal attitudes to innovation free of "red tape", and technological development speed. Six potential GDPR future scenarios are envisioned, ranging from laxer protection than now to models empowering individuals and regulators. While a minor update to the status quo is most likely, I argue a more robust implementation requiring stricter penalties, public censure, cross-border data rights defence, and proactive guidelines for emerging technologies will be necessary.

8.2 Interpretation of results

In the GDPR business paper in Chapter 4, the findings on the negative impacts of the GDPR both support prior predictions and reveal new negatives not considered by the literature. It was widely predicted that the GDPR would increase compliance costs and time-wasting bureaucracy. Our exploratory study extends prior research on these disadvantages with the proviso that the increase in compliance costs was not as high as feared and that the grey areas of law exacerbated the expected bureaucracy. On the other hand, the findings extend prior research on the disadvantages, as no one predicted how it would affect brand development, chill internal communications, and crowd out other worthwhile investments. In particular, no one anticipated the weaponisation of SARs and how disgruntled ex-employees or customers could misuse them as a tool of retaliation.

The findings on benefits confirm many high-level predictions but develop knowledge of cause and effect in more detail. For example, it is no surprise that GDPR raised the profile of data protection. However, I found that privacy consciousness, combined with the threat of large fines, made companies elevate it to the Board level, approve major investments in data management and security and thereby reap modernisation, standardisation and marketing benefits. Companies now have cleaner, more up-to-date customer databases. Without GDPR,

they admit they would still risk collecting, overusing, retaining, and undersecuring data. Similarly, it was well known that the GDPR would require companies to have a DPO and some commentators hypothesised that lawyers would eventually inherit cybersecurity (Woods & Ceross, 2022). However, I find a slightly different situation. Whereas once the compliance department was perceived as populated by box tickers and the information security department as populated by hardware geeks, the need to consider GDPR implications has injected both into conversations hitherto the preserve of the commercial decision-makers. The research found that both relished their newfound influence and were motivated to champion and embed the GDPR within their organisations.

In the GDPR consumer perceptions paper in Chapter 5, the research confirms the trends identified by other surveys that consumer awareness and knowledge of the GDPR has increased since 2018. Surveys have not tested the consumer awareness and knowledge of the regulator. I show the UK regulator's profile is generally low and even lower in the workplace.

The findings in the regulator effectiveness paper in Chaper 6 significantly expand our knowledge and theoretical models of how different stakeholders judge data protection regulator effectiveness. Without well-defined objectives, I find that people (consumers, business executives, NGOs, and regulators) ascribe goals based on their personal motivations and experience. In political science, I discovered it might be characterised as "where you stand depends on where you sit" but my research breaks it down into five data protection-related themes and exposes the granular criteria used in practice. I also extend our understanding of the generic independence-accountability phenomenon by revealing how a weak relationship operates between the DPAs and their political masters on a day-to-day basis and how real pushback relies on inter-DPA and EDPB self-regulation. My findings on current reporting mechanisms show how the legal professions accept practices that seem anachronistic to a technologist. For example, no central incidents databases, no standardised reporting formats and no standardised definitions make transparency and comparability unnecessarily challenging. Finally, I take benchmark theory from business and apply it in an original manner to systematise performance management using KPIs and KPI proxies.

The findings in the futures paper in Chapter 7 bring a fresh perspective to imagining the future shape and evolution of the GDPR because little academic literature exists in this field. Works by scholars (Bradford, 2020, 2023; Carr & Llanos, 2021) tend to be high-level and big picture. Reports by politicians and NGOs (noyb, 2022; Zenner, 2021) are not impartial. Op-eds by journalists are of variable quality. Articles by lawyers are soft marketing. Regulators have to be very careful and measured in their forward-looking statements in case it is perceived to be market sensitive. The paper's significance is the trends it identifies that can be periodically reviewed to discern the future directional space of the GDPR and its well-reasoned predictions of potential scenarios.

8.3 Limitations of the research

A limitation common to the first three papers is the sample size, sampling bias and methodology.

The GDPR business benefits paper in Chapter 4 is based on semi-structured

interviews with 14 executives drawn from six companies in the UK and Ireland. Ideally, it would have benefited from interviewing more executives in more companies in more countries in the EU. It would also have benefited from being able to interview more parallel equivalent-ranking executives in different companies for comparison purposes. The sample size was constrained by the difficulty of recruiting busy senior executives and the fact it happened during the first COVID lockdown. It doesn't make sense for a sample N=14 study to aim to be representative or generalisable, nor does an exploratory study need to be. Nonetheless, given the absence of new themes arising after a dozen interviews, we felt we had hit saturation before the interview round concluded. Regarding sampling bias, all the participants were willing volunteers, which may mean they suffered from social desirability bias. Regarding methodology, the author conducted all the interviews and did the thematic analysis. This can raise concerns about interviewer bias and the decision on saturation. All the interviews and emergent themes were summarised and shared with the supervisors immediately after the meetings to mitigate these concerns.

The GDPR consumer perceptions paper in Chapter 5 is based on a three-stage survey of consumers in the UK who had worked in the same company since before the GDPR became law and, therefore, had seen the changes due to the GDPR first-hand in their own workplace. Ideally, it would have benefited from a larger sample size and participants in the EU zone. The sample size was limited by the funds available and influenced by the power analysis, which showed that the sample size was sufficient. Nevertheless, the generalizability of the findings can be challenged since the UK is no longer in the EU (although the UK GDPR is the same for all intents and purposes). It was considered but introducing additional countries would have introduced additional country-specific complexities with regard to the regulator questions. Regarding sampling bias, participants on Prolific are paid volunteers and may not be representative despite using filters and screening questions to mitigate this known drawback. In terms of methodology, the survey employed a mix of closed Likert and slider scale questions. There were a few open-ended free-text questions. The author did the coding and thematic analysis. Again, this can raise concerns about researcher bias, although the design of the questions and the later statistical analysis were done in conjunction with the supervisors. More generally, closed questions do not offer the richness of open-ended free-text or one-to-one interviews.

The GDPR regulator effectiveness paper in Chapter 6 is based on a large-scale survey of Chief Information Security Officers (CISO) and structured interviews with interviewees with business executives, lawyers, digital rights activists and four national regulators. It is supplemented with an analysis of diverse enforcement databases. A mix of quantitative and qualitative research was used to mitigate prior research limitations. Nonetheless, 23 stakeholder interviews spread across Europe, and only four data protection regulators, which did not include the home UK regulator nor the EU-lead Irish regulator, affected the generalizability of the findings. Regulators are difficult to get on the record at the best of times, and we were pleased we managed to get four (even if the UK and Irish regulators flatly refused to participate). The open-axial coding was done by the author and detailed in the appendix. Nonetheless, this can raise concerns about bias, which suggests a potential larger-scale follow-up would benefit from a multi-researcher approach.

The GDPR futures paper in Chapter 7 is a thought paper. No data was

used for the research described in the paper. The scientific method demands that only what can be proven by quantitative or qualitative data is valid. Thus, regardless of which technique is used—horizon scanning, axes of uncertainty, SWOT or PESTLE analysis—futures studies are characterized by controversies about the status of the field per se. Remember that thinking about the future is not about being right or wrong. It is about considering how numerous plausible future scenarios may impact the GDPR and how it might evolve to cope with them. The future is not written yet. It lies in the choices that are made.

8.4 Implications and contributions

The research has theoretical and practical implications and contributions.

All three research papers have expanded our understanding of the success of the GDPR model and the factors underpinning its support. The threat of fines forced business to invest in modern infrastructure and adopt good data habits, thereby delivering directly and indirectly several tangible and intangible benefits. The imposition of new data practices made employees more demanding of other companies and fostered consumer support for the regulation and the regulator's role. The new powers enjoyed by the regulators under the GDPR brought new responsibility and accountability which I show is under-developed since their objectives and performance measurement are unclear. None of these aspects had been addressed hitherto in detail in the existing literature. The future work is speculative, but since regulators don't speculate publicly, it is a well-informed and reasoned set of predictions similarly lacking in the existing literature.

A practical contribution of the regulator research is the concrete technical and administrative recommendations on organising the reporting of regulator activity to improve accountability. Another is the work on Key Performance Indicators (KPIs) that could be combined to create a balanced scorecard to compare and contrast regulators in future. The practical contribution of the business research is that the deterrence effect of a regulation is heavily dependent on the reality and materiality of the fine i.e. the potential punishment needs to be big enough and likely enough to be taken seriously. The practical contribution of the consumer research is the importance of regulators promoting their own role in the delivery of the regulation's desired outcomes i.e. unaware citizens will not exercise their rights if they are unaware of their rights or the body to go to. The sum of these findings are relevant and applicable to the design of any future regulation in this field.

Regarding potential applications, the most obvious work that could be used and developed is the work on regulator performance assessment. Not only could this be rolled out to all member states in the EU, but it could also (with local customisation) be rolled out to all the other countries that have adopted the GDPR model for their data protection regimes. The lead indicators in the future thinking work could also be reviewed periodically and updated since it will enable business to anticipate the consequences of changes to the GDPR and feed into their risk assessment as well as their strategy and organisational development.

If I expand further beyond the privacy field, the work has revealed that even hard-bitten business people begrudgingly admit that regulation with teeth mod-

ifies their behaviour in ways that can be mutually beneficial for their business and society at large. It is like the corny line from the movie As Good As It Gets when Jack Nickolson says, "You make me want to be a better man," or engaging a personal trainer to compel you to do what you know is good for you. The GDPR provides a good example of how regulation can encourage organisations to do the right thing by default.

This model and the learnings identified in this thesis have applications in other industries. For example, the UK is currently experiencing a crisis in the water industry over sewage spills. Under a Freedom of Information notice in 2023, the FT reported that only one water utility had been fined by the water industry regulator (OFWAT) since the rules came into force in 1994 despite hundreds of thousands of spills in breach of regulations (Hodgson, 2023). Clearly, there is no credible deterrent effect if fines are levied so infrequently for non-compliance.

Moving back from water industries to the digital world, the EU has taken its cue from the GDPR when designing new Acts such as the DSA, DMA and AI Act. The future repercussions of AI, whether positive or negative, are unknowable but could be consequential. To minimise the risk, the EU has attempted to classify AI applications by impact and can impose fines for non-compliance of up to 7 % of global annual turnover per violation for the most serious infringements, or up to 35 million euros, whichever amount is higher. The sanctions system has been modelled after the GDPR fine mechanism, but the EU has gone even further in attempting to deter Big Tech in advance from embarking on projects that are considered dangerous to society. Whether the EU dares to enforce such hefty fines is a different matter, but it does have the power to do so, and often, as the GDPR demonstrates, a credible threat alone may be sufficient.

8.5 Future research directions

The business benefits research outlined in Chapter 4 could be expanded in several directions. Increasing the sample size in the UK & Ireland would increase the representativeness. Specifically, designing the sampling to contain more interviewees with comparable roles and seniority would enable peer comparison of the findings. Similarly, sampling from different industries or countries would enable cross-sector or cross-country comparison. Another avenue could be to study differences in budget and headcount in data compliance since 2018 to see if the GDPR has embedded itself in organisational management structures. This data could also be used to test if sectoral increases in compliance resources were linked to the prevalence and value of fines in those industry sectors.

The consumer perceptions research outlined in Chapter 5 could be repeated to collect longitudinal data for historical analysis and expanded to other countries to facilitate cross-country analysis. It could also be complemented with qualitative research to delve deeper into some of the original research findings, in particular, the idea that people's data protection expectations have risen in the outside world due to having to be more careful with customer data inside their work world.

The regulator effectiveness research in Chapter 6 is ripe for future work as the area is so understudied. Taking the benchmark KPI dashboard and

putting numbers to it is an obvious next step. Some intangible measures, such as perception metrics, would require research to determine the best proxies. Other measures would benefit from the active involvement and collaboration with the EDPB and EDPS to access data sets. This would deliver in-country and cross-country data for analysis and thereby help improve regulator legitimacy, transparency and comparability.

The futures or foresight work in Chapter 7 lends itself to a periodic review where the four key drivers identified in the paper are re-examined to determine what direction in the cone of pathways the GDPR appears to be heading and what that means for decision-makers in business, consumer rights organisations, regulators and policymakers.

8.6 Concluding remarks

This thesis deals with an ongoing struggle facing society. Advances in technology continue to outpace privacy safeguards. Governments and corporations continue to wield unprecedented surveillance capabilities that significantly threaten our fundamental human rights, including the right to privacy. Individuals have tools like PET and legal options to push back, but it is an unequal contest. I explain in the Background Chapter 2 how regulation has traditionally been used to address market failures and power asymmetries. The GDPR is currently regarded as the toughest and most influential regulation to address this power imbalance, which is why I chose to study its effectiveness.

What I have learned is that regulation like the GDPR has well-documented downsides for business, but it also has upsides that business often prefers to underplay (because what businessman wants to encourage more regulation). A new regulation has the potential to impact the power balance within organisations. GDPR gave such a boost to the legal/risk/compliance department. Fines focus the corporate mind. Arguably, the threat of fines of up to 4% of global revenue gave the GDPR an early win. Continued success will depend on the GDPR following through on the threat. Timid enforcement will undermine it. It would appear the EU is convinced the fine structure has potential since it has been copied across to subsequent digital acts. Consumers may be irritated by cookie consent notices, but they take comfort in the fact that the GDPR is on their side. Business appreciates the universality of it across an otherwise multi-domestic market so long as regulators' decisions are proportionate and predictable. National regulators have largely escaped accountability because the single market has long been plagued by national disregard for EU rules, haphazard enforcement, and resistance from capitals to centralising regulatory powers. For the GDPR to succeed going forward, it will require greater political support, period updates to keep pace with technology and judicious exercise of its sanction powers "pour encourager les autres".

I started the PhD program thinking I would research privacy-enhancing technology. I end it by researching privacy-enhancing law. Overall, this thesis deepens our understanding of the GDPR model's success and how it has improved personal data governance, awareness and security. It sheds light on the factors behind the ongoing support from stakeholders. It unpacks their expectations of the regulation and regulator and proposes a framework for evaluating future data protection regulator performance. These studies give the information secu-

rity community a more rounded understanding of the path to protecting privacy at the intersection of technology, business and regulation.

Bibliography

Abbott, K. W., & Snidal, D. (2000). Hard and Soft Law in International Governance. *International Organization*, *54*(3), 421–456. Retrieved March 21, 2023, from https://www.jstor.org/stable/2601340

Abbott, K. W., & Snidal, D. (2013). Taking responsive regulation transnational: Strategies for international organizations. *Regulation & Governance*, *7*(1), 95–113. doi: 10.1111/j.1748-5991.2012.01167.x

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: Examining user scenarios and privacy preferences. *Proceedings of the 1st ACM conference on Electronic commerce - EC '99*, 1–8. doi: 10.1145/336992.336995

ACLU. (2013). NSA Documents Released to the Public Since June 2013. Retrieved November 4, 2024, from https://www.aclu.org/nsa-documents-released-to-the-public-since-june-2013

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy*, *3*(1), 26–33. doi: 10.1109/MSP.2005.22

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM conference on Electronic commerce*, 21–29. doi: 10.1145/988772.988777

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. doi: 10.1126/science.aaa1465

Acquisti, A., & Grossklags, J. (2003). Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. http://www.infosecon.net/workshop/downloads/2003/pdf/Final_session6_acquisti.pdf

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies*, *42*(2), 249–274. doi: 10.1086/671754

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, *54*(2), 442–492. doi: 10.1257/jel.54.2.442

Addis, M., & Kutar, M. (2018). The General Data Protection Regulation (GDPR), Emerging Technologies and UK Organisations: Awareness, Implementation and Readiness. *UK Academy for Information Systems Conference Proceedings 2018*. https://aisel.aisnet.org/ukais2018/29

Agarwal, S. (2016). Towards dealing with GDPR uncertainty. *11th IFIP Summer School on Privacy and Identity Management*, 1–7. Retrieved May

30, 2021, from https://docplayer.net/124763164-Towards-dealing-with-gdpr-uncertainty.html

Aguilar, F. J. (1967). *Scanning the business environment*. Macmillan.

Allen, D. W. E., Berg, A., Berg, C., Markey-Towler, B., & Potts, J. (2019). Some Economic Consequences of the GDPR. *Economics Bulletin*, *39*(2), 785–797. doi: 10.2139/ssrn.3160404

Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). The critical success factors of GDPR implementation: A systematic literature review. *Digital Policy, Regulation and Governance*, *21*(4), 402–418. doi: 10.1108/DPRG-01-2019-0007

Anand, N., & Brass, I. (2021). Responsible innovation for digital identity systems. *Data & Policy*, *3*. doi: 10.1017/dap.2021.35

Anita R. Gohdes. (2020). Repression Technology: Internet Accessibility and State Violence - Gohdes - 2020 - American Journal of Political Science - Wiley Online Library. https://onlinelibrary.wiley.com/doi/full/10.1111/ajps.12509

Arner, D. W., Castellano, G. G., & Selga, E. K. (2022). The Transnational Data Governance Problem. *Berkeley Technology Law Journal*, *37*(2), 623–700. https://heinonline.org/HOL/P?h=hein.journals/berktech37&i=666

Arora, P. (2016). Bottom of the Data Pyramid: Big Data and the Global South. *International Journal of Communication*, *10*(0), 19. https://ijoc.org/index.php/ijoc/article/view/4297

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Retrieved March 25, 2022, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Ayres, I., & Braithwaite, J. (1992). *Responsive Regulation: Transcending the Deregulation Debate*. Oxford University Press.

Baek, Y. M., Kim, E.-m., & Bae, Y. (2014). My privacy is okay, but theirs is endangered: Why comparative optimism matters in online privacy concerns. *Computers in Human Behavior*, *31*, 48–56. doi: 10.1016/j.chb.2013.10.010

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding regulation: Theory, strategy, and practice* (2nd ed). Oxford University Press.

Banks, M. (2018). *Using Visual Data in Qualitative Research*. SAGE.

Barnard-Wills, D. D., Cochrane, L., Matturi, M. K., & Marchetti, D. F. (2019). Report on the SME experience of the GDPR Version 1.0. https://trilateralresearch.com/wp-content/uploads/2020/01/STAR-II-D2.2-SMEs-experience-with-the-GDPR-v1.0-.pdf

Barnes, J., & Burke, T. F. (2012). Making Way: Legal Mobilization, Organizational Response, and Wheelchair Access. *Law & Society Review*, *46*(1), 167–198. doi: 10.1111/j.1540-5893.2012.00476.x

Battista, M. (2024). CIPD — PESTLE analysis. https://www.cipd.org/uk/knowledge/factsheets/pestle-analysis-factsheet/

Bawn, K. (1995). Political Control Versus Expertise: Congressional Choices about Administrative Procedures. *American Political Science Review*, *89*(1), 62–73. doi: 10.2307/2083075

Bawn, K. (1997). Choosing Strategies to Control the Bureaucracy: Statutory Constraints, Oversight, and the Committee System. *The Journal of Law, Economics, and Organization*, *13*(1), 101–126. doi: 10.1093/oxfordjournals.jleo.a023375

Beckett, P. (2017). GDPR compliance: Your tech department's next big opportunity. *Computer Fraud & Security*, *2017*(5), 9–13. doi: 10.1016/S1361-3723(17)30041-6

Belgian DPA. (2021). *The Belgian DPA publishes its annual report 2020* (tech. rep.). https://www.dataprotectionauthority.be/the-belgian-dpa-publishes-its-2020-annual-report

Bennett, C. J. (2018). The European General Data Protection Regulation: An instrument for the globalization of privacy standards? (S. A. Chun, N. R. Adam, & B. Noveck, Eds.). *IP*, *23*(2), 239–246. doi: 10.3233/IP-180002

Black, J. (2005). The emergence of risk-based regulation and the new public management in the United Kingdom. *Public Law*, *2005*(Autumn), 512–549. http://www.sweetandmaxwell.co.uk/Catalogue/ProductDetails.aspx?recordid=469

Black, J. (2007). Principles based regulation: Risks, challenges and opportunities. http://www.supremecourt.justice.nsw.gov.au/

Black, J., & Kingsford, S. D. (2002). Critical reflections on regulation [Plus a reply by Dimity Kingsford Smith.] *Australasian Journal of Legal Philosophy*, *27*(2002), 1–46. doi: 10.3316/ielapa.200206927

Bornschein, R., Schmidt, L., & Maier, E. (2020). The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices. *Journal of Public Policy and Marketing*, *39*(2), 135–154. doi: 10.1177/0743915620902143

Boult, M. (2018). *Horizon scanning: A practitioner's guide* (tech. rep.). Institute of Risk Management. https://pure.roehampton.ac.uk/ws/portalfiles/portal/1155531/Horizon_scanning_final2.pdf

Bowden, C. (2014). The Cloud Conspircay. https://media.ccc.de/v/31c3_-_6195_-_en_-_saal_g_-_201412272145_-_the_cloud_conspiracy_2008-2014_-_caspar_bowden/playlist

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

Bradford, A. (2023). *Digital Empires: The Global Battle to Regulate Technology*. Oxford University Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. doi: 10.1191/1478088706qp063oa

Breyer, S. (1982). *Regulation and Its Reform*. Harvard University Press.

Briefing, C. (2022). PIPL vs GDPR - Key Differences and Implications for Compliance in China. Retrieved February 4, 2024, from https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/

Broadbent, M. (2020). The Digital Services Act, the Digital Markets Act, and the New Competition Tool. https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool

Brunton, F., & Nissenbaum, H. F. (2015). *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press. doi: 10.7551/mitpress/9780262029735.001.0001

Buck, C., Horbel, C., Germelmann, C. C., & Eymann, T. (2014). The unconscious app consumer: Discovering and comparing the information seeking patterns among mobile application consumers. *ECIS 2014 Proceedings*. https://aisel.aisnet.org/ecis2014/proceedings/track14/8

Buckley, G., Caulfield, T., & Becker, I. (2022). 'It may be a pain in the backside but...' Insights into the resilience of business after GDPR. *New Security Paradigms Workshop (NSPW '22)*, 21–34. doi: 10.1145/3584318.3584320

Buckley, G., Caulfield, T., & Becker, I. (2024a). GDPR and the indefinable effectiveness of privacy regulators: Can performance assessment be improved? *Journal of Cybersecurity*, *10*(1). doi: 10.1093/cybsec/tyae017

Buckley, G., Caulfield, T., & Becker, I. (2024b). GDPR: Is it worth it? Perceptions of workers who have experienced its implementation. doi: 10.48550/arXiv.2405.10225

Buckley, G., Caulfield, T., & Becker, I. (2024c). How might the GDPR evolve? A question of politics, pace and punishment. *Computer Law & Security Review*, *54*. doi: 10.1016/j.clsr.2024.106033

Carpenter, D. (2001). The Political Foundations of Bureaucratic Autonomy: A Response to Kernell. *Studies in American Political Development*, *15*(1), 113–122. doi: 10.1017/S0898588X01010069

Carpenter, D. P., & Krause, G. A. (2012). Reputation and Public Administration. *Public Administration Review*, *72*(1), 26–32. doi: 10.1111/j.1540-6210.2011.02506.x

Carr, M., & Llanos, J. T. (2021). Data: Global governance challenges. In *Global Governance Futures* (pp. 238–252). Routledge. doi: 10.4324/9781003139836-21

Chazal, E. d. (2024). 20 Biggest GDPR Fines 2018 - 2024 — Breaches of GDPR — Skillcast. Retrieved October 7, 2024, from https://www.skillcast.com/blog/20-biggest-gdpr-fines

Ciriani, S. (2015). The Economic Impact of the European Reform of Data Protection. *Communications & Strategies*, *97*, 41–58. Retrieved May 29, 2021, from https://papers.ssrn.com/abstract=2674010

CJEU. (2015). The CJEU's Schrems ruling on the Safe Harbour Decision — Think Tank — European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2015)569050

CJEU. (2020). The CJEU judgment in the Schrems II case. https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf

Cloud, M. (2018). Property Is Privacy: Locke and Brandeis in the Twenty-First Century Symposium: Katz @ 50: The Fourth Amendment in the Digital Age. *American Criminal Law Review*, *55*(1), 37–76. https://heinonline.org/HOL/P?h=hein.journals/amcrimlr55&i=43

CMS Germany. (2023). GDPR Enforcement Tracker - list of GDPR fines. https://www.enforcementtracker.com

Cochrane, L., Jasmontaite-Zaniewicz, L., & Barnard-Wills, D. (2020). Data Protection Authorities and their Awareness-raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate

Guidance for Small and Medium-size Enterprises. *European Data Protection Law Review*, *6*(3), 352–364. doi: 10.21552/edpl/2020/3/6

Coglianese, C. (2012). *Measuring Regulatory Performance: Evaluating the impact of regulation and regulatory policy* (tech. rep.). https://www.oecd.org/regreform/regulatory-policy/1_coglianese%20web.pdf

Coglianese, C., & Lazer, D. (2003). Management-Based Regulation: Prescribing Private Management to Achieve Public Goals. *Law & Society Review*, *37*(4), 691–730. doi: 10.1046/j.0023-9216.2003.03703001.x

Commission, E. (2018). Context analysis – PESTEL. https://wikis.ec.europa.eu/pages/viewpage.action?pageId=50109048

Commission, E. (2020). Communication from the Commission to the European Parliament and the Council. doi: 10.1163/2210-7975_HRD-4679-0058

Cooper, D., Meneses, A., & Choi, S. (2023). European Commission Plans to Improve Cooperation Between Supervisory Authorities in Cross-Border GDPR Cases. https://www.insideprivacy.com/gdpr/european-commission-plans-to-improve-cooperation-between-supervisory-authorities-in-cross-border-gdpr-cases/

Cordes, J. J., Dudley, S. E., & Washington, L. Q. (2022). *Regulatory Compliance Burdens Literature Review & Synthesis* (tech. rep.). The George Washington University Regulatory Studies Center. https://regulatorystudies.columbian.gwu.edu/sites/g/files/zaxdzs4751/files/2022-10/regulatory_compliance_burdens_litreview_synthesis_finalweb.pdf

Cornell Law school. (n.d.). Privacy. https://www.law.cornell.edu/wex/privacy

Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New Media & Society*, *20*(1), 88–104. doi: 10.1177/1461444816657096

CRSP. (2024). Market Indexes – Center for Research in Security Prices. https://www.crsp.org/indexes/

Dataguard. (2022). Data Protection Officer salary: Costs for an external or internal DPO. Retrieved February 23, 2022, from https://www.dataguard.co.uk/blog/data-protection-officer-salary-costs-for-an-external-or-internal-dpo

Davies, D. (2019). Understanding Regulation - Regulatory Failure - Examples. https://www.regulation.org.uk/ob-regulatory_failure-examples.html

Davies, T. (1999). Recovering the Original Fourth Amendment. *Michigan Law Review*, *98*(3), 547–750. https://repository.law.umich.edu/mlr/vol98/iss3/2

Davis, D. T., Owen. (2024). U.S. Privacy Litigation Update: June 2024. Retrieved January 28, 2025, from https://www.bytebacklaw.com/2024/07/u-s-privacy-litigation-update-june-2024/

De Hert, P. (2021). EU sanctioning powers and data protection: New tools for ensuring the effectiveness of the GDPR in the spirit of cooperative federalism.

De Hert, P., & Papakonstantinou, V. (2015). The data protection regime in China. *European Parliament*. https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA%282015%29536472_EN.pdf

De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., & Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer Law & Security Review*, *34*(2), 193–203. doi: 10.1016/j.clsr.2017.10.003

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83–108. doi: 10.1111/j.1083-6101.2009.01494.x

Defense, C. A. (2025). Trend #3 – Privacy Class Actions Continue To Proliferate As Plaintiffs Search For Winning Theories [Section: Duane Morris Class Action Review – 2025]. https://blogs.duanemorris.com/classactiondefense/2025/01/13/trend-3-privacy-class-actions-continue-to-proliferate-as-plaintiffs-search-for-winning-theories/

Dellie, L. (2019). *GDPR Compliance as a Competitive Advantage*. ISACA. Retrieved May 28, 2021, from https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2019/gdpr-compliance-as-a-competitive-advantage

Deloitte. (2018). *GDPR six months on*. London, UK. Retrieved April 8, 2021, from https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf

Dettling, L. (2024). Tech Policy Trends 2024: The evolution of GDPR. https://accesspartnership.com/tech-policy-trends-2024-the-evolution-of-gdpr/

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. doi: 10.1287/isre.1060.0080

DLA Piper. (2022). *DLA Piper GDPR fines and data breach survey: January 2022 — Insights — DLA Piper Global Law Firm* (tech. rep.). Retrieved February 17, 2022, from https://www.dlapiper.com/en/uk/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/

Donn, P. (2023). GDPR 5 years on. Retrieved April 22, 2024, from https://dpnetwork.org.uk/gdpr-5-years-on/

Dove, E. S. (2018). The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era. *J Law Med Ethics*, *46*(4), 1013–1030. doi: 10.1177/1073110518822003

DPC. (2023). Data Protection Commission Annual Report 2022. https://www.dataprotection.ie/sites/default/files/uploads/2023-03/DPC%20AR%20English_web.pdf

DPP. (2024). Five Years of Data Protection Evolution. https://dataprotectionpeople.com/resource-centre/five-years-of-data-protection-evolution/

Draper, N. A. (2017). From Privacy Pragmatist to Privacy Resigned: Challenging Narratives of Rational Choice in Digital Privacy Debates. *Policy & Internet*, *9*(2), 232–251. doi: 10.1002/poi3.142

Drucker, P. (2016). *The Effective Executive*. Routledge. doi: 10.4324/9780080549354

Dubrova, D. (2018). *Challenges and Benefits of GDPR Implementation*. The App Solutions. Retrieved April 20, 2021, from https://theappsolutions.com/blog/development/gdpr-challenges-and-benefits/

EC. (1995). The Data Protection Directive 1995 [Type: text/html; charset=UTF-8]. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A31995L0046

EC. (2023a). Data Act — Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/data-act

EC. (2023b). Commission welcomes political agreement on Artificial Intelligence Act — Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-artificial-intelligence-act

EC. (2024a). The Digital Markets Act: Ensuring fair and open digital markets - European Commission. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

EC. (2024b). The EU's Digital Services Act. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

EC. (2024c). Proposal for an ePrivacy Regulation — Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation

EDPB. (2021). *Report 2021 Overview on resources and enforcement* (tech. rep.). https://edpb.europa.eu/system/files/2021-08/edpb_report_2021_overviewsaressourcesandenforcement_v3_en_0.pdf

EDPB. (2022). *Report 2022 Overview on resources and enforcement* (tech. rep.). https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf

Edward Snowden. (2015). Snowden Archive. https://www.cjfe.org/snowden

Eggers, D. (2013). *The Circle*. Knopf Doubleday Publishing Group.

Eggers, D. (2021). *The Every*. Knopf Doubleday Publishing Group.

Éireann, S. (2023). Courts and Civil Law (Miscelaneous Provisions) Bill 2022. https://data.oireachtas.ie/ie/oireachtas/bill/2022/84/seanad/3/amendment/numberedList/eng/b84b22d-scnl.pdf

Emch, A. (2019). Antitrust and the Internet: Is China Different. *Competition Law International*, *15*(2), 167–174. https://heinonline.org/HOL/P?h=hein.journals/cmpetion15&i=165

EO. (2022). Decision on whether the European Commission collects sufficient information to monitor Ireland's implementation of the EU's General Data Protection Regulation (GDPR) (Case 97/2022/PB) — Decision — European Ombudsman. Retrieved March 23, 2023, from https://www.ombudsman.europa.eu/en/decision/en/164337

Espinoza, J. (2021). Fighting in Brussels bogs down plans to regulate Big Tech. *Financial Times*. https://www.ft.com/content/7e8391c1-329e-4944-98a4-b72c4e6428d0

EU. (2018a). Art. 1 GDPR – Subject-matter and objectives. https://gdpr-info.eu/art-1-gdpr/

EU. (2018b). Art. 1 GDPR – Subject-matter and objectives. https://gdpr-info.eu/art-1-gdpr/

EU. (2018c). Art. 51 GDPR – Supervisory authority. https://gdpr-info.eu/art-51-gdpr/

EU. (2018d). Art. 57 GDPR – Tasks. Retrieved June 16, 2023, from https://gdpr-info.eu/art-57-gdpr/

EU. (2018e). Art. 58 GDPR – Powers. Retrieved March 23, 2023, from https://gdpr-info.eu/art-58-gdpr/

EU. (2018f). Art. 59 GDPR – Activity reports. Retrieved March 23, 2023, from https://gdpr-info.eu/art-59-gdpr/

EU. (2018g). Art. 68 GDPR – European Data Protection Board. Retrieved March 23, 2023, from https://gdpr-info.eu/art-68-gdpr/

EU. (2018h). General Data Protection Regulation (GDPR) – Official Legal Text. https://gdpr-info.eu/

EU DMA. (2022). The Digital Markets Act: Ensuring fair and open digital markets [Type: Text]. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

EUR-Lex. (2002). Precautionary principle - EUR-Lex. https://eur-lex.europa.eu/EN/legal-content/glossary/precautionary-principle.html

EUR-Lex. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)Text with EEA relevance. Retrieved July 16, 2024, from http://data.europa.eu/eli/reg/2024/1689/oj/eng

European Commission. (2019). *General Data Protection Regulation one year on* (Press Release No. IP/19/2956). Retrieved June 21, 2021, from https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2956

European Commission. (2023). Further specifying procedural rules relating to the enforcement of the General Data Protection Regulation - Have your say. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13745-Further-specifying-procedural-rules-relating-to-the-enforcement-of-the-General-Data-Protection-Regulation_en

European Commission, Directorate General for Justice and Consumers. (202023). *EU: Multistakeholder Experts Group publishes contribution on GDPR evaluation*. DataGuidance. Retrieved April 8, 2021, from https://www.dataguidance.com/news/eu-multistakeholder-experts-group-publishes

European Commission. Directorate General for Justice and Consumers. & Kantar. (2019). *The General Data Protection Regulation: Report.* (tech. rep.). Publications Office. LU. Retrieved February 15, 2022, from https://data.europa.eu/doi/10.2838/43726

European Data Protection Board. (2023). EDPB Work Programme 2023/2024. https://edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf

European Digital Rights. (2022). EDRI letter to EDPB. https://noyb.eu/sites/default/files/2022-09/EDRI_LETER_TO_EDPB.pdf

European Parliament and of the Council. (2016). Regulation (EU) 2016/679. *Official Journal of the European Union*, *119*(1). Retrieved May 29, 2021, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

European Parliament. Directorate General for Internal Policies. (2012). *Fighting cyber crime and protecting privacy in the cloud* (tech. rep.). https://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET%282012%29462509_EN.pdf

European Parliament. Directorate General for Parliamentary Research Services. (2019). *Blockchain and the general data protection regulation: Can dis-*

tributed ledgers be squared with European data protection law? Publications Office. https://data.europa.eu/doi/10.2861/535

European Parliament. Directorate General for Parliamentary Research Services. (2020). *The impact of the general data protection regulation on artificial intelligence.* Publications Office. https://data.europa.eu/doi/10.2861/293

European Union. (2022). General data protection regulation (GDPR). https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html

Faverio, M. (2023). Key findings about Americans and data privacy. https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/

Fimin, M. (2018). Council Post: Five Benefits GDPR Compliance Will Bring To Your Business [magazine]. *Forbes*. Retrieved May 30, 2021, from https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/

Fisk, J. (2023). EU-US Data Privacy Framework: 3rd time lucky? Retrieved February 6, 2024, from https://www.dpocentre.com/eu-us-data-privacy-framework-3rd-time-lucky/

Fiveash, K. (2014). Viv Reding: That French Google fine? Pfft - it's pocket money. https://www.theregister.com/2014/01/21/viviane_reding_says_google_cnil_fine_is_pocket_money/

Fool, M. (2024). The Surprising Truth About the S&P 500 and the "Magnificent 7" in 2024. https://foolwealth.com/insights/sp500-and-the-magnificent-7-in-2024

for Fundamental Rights, E. U. A. (2015). Article 8 - Protection of personal data. http://fra.europa.eu/en/eu-charter/article/8-protection-personal-data

Ford, A., Al-Nemrat, A., Ghorashi, S. A., & Davidson, J. (2021). The Impact of GDPR Infringement Fines on the Market Value of Firms. *European Conference on Cyber Warfare and Security*, 473–481, XI. doi: https://doi.org/10.34190/EWS.21.088

FRA. (2009). Article 8 - Protection of personal data — European Union Agency for Fundamental Rights. https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data

Freitas, M. d. C., & Mira da Silva, M. (2018). GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*, *3*(4). doi: 10.20897/jisem/3941

Fuster, G. G., Ausloos, J., Bons, D., Bygrave, L. A., Drechsler, L., Gkotsopoulou, O., Hristov, C., Irion, K., Kroese, C., Lynskey, O., & Magierska, M. (2022). An empirical study of current practices under the GDPR.

Garber, J. (2018). GDPR – compliance nightmare or business opportunity? *Computer Fraud & Security*, *2018*(6), 14–15. doi: 10.1016/S1361-3723(18)30055-1

Gasser, U. (2016). Recoding Privacy Law: Reflections on the Future Relationship among Law, Technology, and Privacy. *Harvard Law Review Forum*, *130*, 61. https://heinonline.org/HOL/Page?handle=hein.journals/forharoc130&id=62&div=&collection=

GDPR.eu. (2018). What are the GDPR Fines? https://gdpr.eu/fines/

GDPR.eu. (2019). *GDPR Small Business Survey*. Proton Technologies AG. Retrieved May 29, 2021, from https://gdpr.eu/2019-small-business-survey/

Gentile, G., & Lynskey, O. (2022). Deficient by design? The tansnational enforcement of the GDPR. *International & Comparative Law Quarterly*, *71*(4), 799–830. doi: 10.1017/S0020589322000355

Gilardi, F. (2002). Policy credibility and delegation to independent regulatory agencies: A comparative empirical analysis. *Journal of European Public Policy*, *9*(6), 873–893. doi: 10.1080/1350176022000046409

Gormley, W. T. (1986). Regulatory Issue Networks in a Federal System. *Polity*, *18*(4), 595–620. doi: 10.2307/3234884

Government Office for Science. (2020). *The future of citizen data systems* (tech. rep.).

GOV.UK. (2017). The Futures Toolkit: Tools for Futures Thinking and Foresight across UK Government. *Government Office for Science*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/674209/futures-toolkit-edition-1.pdf

Grant, H., & Crowther, H. (2016). How Effective Are Fines in Enforcing Privacy? In D. Wright & P. De Hert (Eds.), *Enforcing Privacy: Regulatory, Legal and Technological Approaches* (pp. 287–305). Springer International Publishing. doi: 10.1007/978-3-319-25047-2_13

Great Britain & Information Commissioner's Office. (2021). *Information Commissioner's Annual Report and Financial Statements 2020-21*.

Guest, G., MacQueen, K. M., & Namey, E. E. (2011). *Applied Thematic Analysis*. SAGE Publications.

Guest, G., Namey, E., & Chen, M. (2020). A simple method to assess and report thematic saturation in qualitative research. *PLOS ONE*, *15*(5), e0232076. doi: 10.1371/journal.pone.0232076

Gunningham, N., Kagan, R. A., & Thornton, D. (2004). Social License and Environmental Protection: Why Businesses Go Beyond Compliance. *Law & Social Inquiry*, *29*(2), 307–341. doi: 10.1111/j.1747-4469.2004.tb00338.x

Hahn, R. W., & Dudley, P. M. (2004). How Well Does the Government Do Cost-Benefit Analysis? [Place: Rochester, NY Type: SSRN Scholarly Paper]. doi: 10.2139/ssrn.495462

Hartzog, W. (2018). *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Harvard University Press.

Hernández, J. G. (2024). Future privacy rules for a Digital EU. Retrieved April 22, 2024, from https://www.telefonica.com/en/communication-room/blog/future-privacy-rules-for-a-digital-eu/

Herzberg, F., Mausner, B., & Snyderman, B. B. (2017). *The Motivation to Work* (1st ed.). Routledge. https://doi.org/10.4324/9781315124827

Hijmans, H. (2018). How to Enforce the GDPR in a Strategic, Consistent and Ethical Manner Discussion. *European Data Protection Law Review (EDPL)*, *4*(1), 80–84. Retrieved February 23, 2022, from https://heinonline.org/HOL/P?h=hein.journals/edpl4&i=86

Hille, K. (2023). 'Like it was with Jack Ma': China puts world's biggest Apple supplier in its crosshairs [Section: Foxconn Technology Group]. *Financial Times*. Retrieved February 19, 2024, from https://www.ft.com/content/47903211-8fbe-49ac-8f15-c3d9aa098397

Hirvelä, P., & Heikkilä, S. (2022). *Right to Respect for Private and Family Life, Home and Correspondence: A Practical Guide to the Article 8 Case-Law of the European Court of Human Rights* (1st ed.). Intersentia. doi: 10.1017/9781839703232

Hodges, C. (2018). Delivering Data Protection: Trust and Ethical Culture Discussion. *European Data Protection Law Review (EDPL)*, *4*(1), 65–79. Retrieved February 23, 2022, from https://heinonline.org/HOL/P?h=hein.journals/edpl4&i=71

Hodgson, C. (2023). Ofwat has fined just one water company over 1994 sewage spill rules [Section: Water Services Regulation Authority UK]. *Financial Times*. https://www.ft.com/content/95a62770-c6f4-4cbc-ad90-495e5803d232

Hodgson, C., & Kinder, T. (2024). Microsoft's and Google's AI plans clouded by concerns of rising costs [Section: Microsoft Corp]. *Financial Times*. https://www.ft.com/content/a062df1d-aaf5-4604-8f97-4444170482f2

Hoepman, J.-H. (2021). *Privacy Is Hard and Seven Other Myths: Achieving Privacy through Careful Design*. MIT Press.

Holvast, J. (2007). 27 - History of privacy. In K. D. Leeuw & J. Bergstra (Eds.), *The History of Information Security* (pp. 737–769). Elsevier Science B.V. doi: 10.1016/B978-044451608-4/50028-6

Hood, C. (2007). What happens when Transparency meets Blame Avoidance. https://www.regulation.org.uk/library/2007-Christopher_Hood-What_happens_when_Transparency_meets_Blame_Avoidance.pdf

H.R.4943: 115th Congress (2017-2018). (2018). CLOUD Act. Retrieved February 4, 2024, from https://www.congress.gov/bill/115th-congress/house-bill/4943

IAPP. (2021). Standing issues in U.S. privacy class actions — IAPP. https://iapp.org/news/a/standing-issues-in-u-s-privacy-class-actions

ICO. (2018a). Dp-act-12-steps-infographic.pdf. Retrieved February 21, 2022, from https://ico.org.uk/media/for-organisations/documents/2014918/dp-act-12-steps-infographic.pdf

ICO. (2018b). Preparing for the law enforcement requirements (part 3) of the Data Protection Act 2018: https://ico.org.uk/media/for-organisations/documents/2014918/dp-act-12-steps-infographic.pdf

ICO. (2024). How can PETs help with data protection compliance? [Publisher: ICO]. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/how-can-pets-help-with-data-protection-compliance/

Interesse, G. (2023). A Comprehensive Analysis of the European GDPR and Evolving Chinese Data Protection Laws. Retrieved February 6, 2024, from https://www.europeanguanxi.com/post/a-comprehensive-analysis-of-the-european-gdpr-and-evolving-chinese-data-protection-laws

International, A. (2023). Ireland: Draconian law to make data protection procedures confidential. https://www.amnesty.org/en/latest/news/2023/06/ireland-draconian-law-to-make-data-protection-procedures-confidential/

Intersoft Consulting. (2018). General Data Protection Regulation (GDPR) – Official Legal Text. Retrieved February 28, 2022, from https://gdpr-info.eu/

IPSOS. (2022). Internet users' trust in the Internet has dropped significantly since 2019 — Ipsos. https://www.ipsos.com/en/trust-in-the-internet-2022

Irish Council for Civil Liberties. (2023). *5-years: GDPR's crisis point* (tech. rep.). Retrieved May 17, 2023, from https://www.iccl.ie/wp-content/uploads/2023/05/5-years-GDPR-crisis.pdf

Isaacson, W. (2012). The Real Leadership Lessons of Steve Jobs [Section: Innovation]. *Harvard Business Review*. https://hbr.org/2012/04/the-real-leadership-lessons-of-steve-jobs

ITIF. (2021). How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime — ITIF. https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data/

Jasmontaitė-Zaniewicz, L., Calvi, A., Nagy, R., & Barnard-Wills, D. (Eds.). (2021). *The GDPR made simple(r) for SMEs*. ASP editions - Academic; Scientific Publishers. doi: 10.46944/9789461171092

Jin, G. Z., & Wagman, L. (2019). *Big Data at the Crossroads of Antitrust and Consumer Protection* (SSRN Scholarly Paper No. ID 3754671). Social Science Research Network. Rochester, NY. https://papers.ssrn.com/abstract=3754671

Johnson, G. (2022). Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond. https://www-nber-org.libproxy.ucl.ac.uk/papers/w30705

Jonker, J., & Pennink, B. (2010). *The Essence of Research Methodology: A Concise Guide for Master and PhD Students in Management Science*. Springer Science & Business Media.

Joskow, P. L., & Rose, N. L. (1989). Chapter 25 The effects of economic regulation. In *Handbook of Industrial Organization* (pp. 1449–1506, Vol. 2). Elsevier. doi: 10.1016/S1573-448X(89)02013-3

Kaushik, W. (2018). *Data Privacy: Demystifying The GDPR*. iSchool — Syracuse University. Retrieved June 21, 2021, from https://ischool-dev.syr.edu/data-privacy-demystifying-gdpr/

Keefer, P., & Stasavage, D. (2002). Checks and Balances, Private Information, and the Credibility of Monetary Commitments. *International Organization*, *56*(4), 751–774. doi: 10.1162/002081802760403766

Kehr, F., Wentzel, D., & Kowatsch, T. (2014). Privacy Paradox Revised: Pre-Existing Attitudes, Psychological Ownership, and Actual Disclosure, 1–15. http://aisel.aisnet.org/icis2014/proceedings/ISSecurity/18/

Kehr, F., Wentzel, D., & Mayer, P. (2013). Rethinking the Privacy Calculus: On the Role of Dispositional Factors and Affect [Type: Forthcoming]. https://www.alexandria.unisg.ch/224696/

Ken Gormley. (1992). One Hundred Years of Privacy. https://heinonline.org/HOL/Page?handle=hein.journals/wlr1992&div=57&g_sent=1&casa_token=&collection=journals

Kessler, J. (2019). Data Protection in the Wake of the GDPR: California's Solution for Protecting "the World's Most Valuable Resource" Notes. *S. Cal. L. Rev.*, *93*(1), 99–128. Retrieved May 29, 2021, from https://heinonline.org/HOL/P?h=hein.journals/scal93&i=109

Khan, J. (2018). The need for continuous compliance. *Network Security*, *2018*(6), 14–15. doi: 10.1016/S1353-4858(18)30057-6

Klosowski, T. (2021). The State of Consumer Data Privacy Laws in the US (And Why It Matters). Retrieved January 28, 2025, from https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, *3*(4), 222–228. doi: 10.1093/idpl/ipt017

Koops, B.-J., Newell, B. C., Timan, T., Skorvanek, I., Chokrevski, T., & Galic, M. (2016). A Typology of Privacy. *University of Pennsylvania Journal of International Law*, *38*(2), 483–576. https://heinonline.org/HOL/P?h=hein.journals/upjiel38&i=489

Koski, H., & Valmari, N. (2020). *Short-term Impacts of the GDPR on Firm Performance* (Working Paper No. 77). ETLA Working Papers. Retrieved July 16, 2024, from https://www.econstor.eu/handle/10419/237362

Krikke, J., Valgaeren, E., & Origer, G. (2019). *GDPR: What are the challenges?* Stibbe. Retrieved May 30, 2021, from https://www.stibbe.com/en/expertise/practiceareas/data-protection/general-data-protection-regulation/what-are-the-challenges

Kumaraguru, P., & Cranor, L. (2005). *Privacy indexes: A survey of Westin's studies* (Technical Report No. 856). Carnegie-Mellon University. http://repository.cmu.edu/isr/856

Kuner, C., Bygrave, L. A., Docksey, C., Drechsler, L., & Tosoni, L. (2021). The EU General Data Protection Regulation: A Commentary/Update of Selected Articles [Place: Rochester, NY Type: SSRN Scholarly Paper]. doi: 10.2139/ssrn.3839645

Kuran, T. (1997). *Private Truths, Public Lies: The Social Consequences of Preference Falsification*. Harvard University Press.

Larsson, A., & Lilja, P. (2019). GDPR: What are the risks and who benefits? In *The Digital Transformation of Labor (Open Access): Automation, the Gig Economy and Welfare* (pp. 187–199). doi: 10.4324/9780429317866-11

Law, Y. (2024). Top Class Action Cases Of 2024: Key Highlights And Insights [Section: News]. Retrieved January 31, 2025, from https://young-lawgroup.com/news/top-class-action-cases-of-2024/

Lawne, R. (2023). GDPR vs U.S. state privacy laws: How do they measure up? https://www.fieldfisher.com/en/insights/gdpr-vs-u-s-state-privacy-laws-how-do-they-measure

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, *71*(9), 862–877. doi: 10.1016/j.ijhcs.2013.01.005

Levy, S. (2014). Hackers at 30: "Hackers" and "Information Wants to Be Free". *Wired*. https://www.wired.com/story/hackers-at-30-hackers-and-information-wants-to-be-free/

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. doi: 10.1080/1097198X.2019.1569186

Lindgren, P. (2016). GDPR Regulation Impact on Different Business Models and Businesses. *Journal of Multi Business Model Innovation and Technology*, *4*(3), 241–254. doi: 10.13052/jmbmit2245-456X.434

Liu, L. (2021). The Rise of Data Politics: Digital China and the World. *Studies in Comparative International Development*, *56*(1), 45–67. doi: 10.1007/s12116-021-09319-8

Liu, Q. (2023). China to lay down AI rules with emphasis on content control [Section: Artificial intelligence]. *Financial Times*. Retrieved February 19, 2024, from https://www.ft.com/content/1938b7b6-baf9-46bb-9eb7-70e9d32f4af0

Locke, J. (1689). *Two Treatises of Government* (1st edition). CreateSpace Independent Publishing Platform.

Lomas, N. (2023). Big changes coming for GDPR enforcement on Big Tech in Europe? *TechCrunch*. https://techcrunch.com/2023/01/31/gdpr-enforcement-reform-dpa-oversight/

Lopes, I. M., & Oliveira, P. (2018). Implementation of the general data protection regulation: A survey in health clinics. *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6. doi: 10.23919/CISTI.2018.8399156

Lynskey, O. (2014). Deconstructing data protection: The 'added-value' of a right to data protection in the EU legal order. *International & Comparative Law Quarterly*, *63*(3), 569–597. doi: 10.1017/S0020589314000244

Lynskey, O. (2023). Complete and effective data protection. *Current Legal Problems*, *76*(1), 297–344. https://academic.oup.com/clp

Lyon, D. (2007). *Surveillance Studies: An Overview*. Polity.

MacAskill, E., Dance, G., Cage, F., Chen, G., & Popovich, N. (2013). NSA files decoded: Edward Snowden's surveillance revelations explained [Section: US news]. *the Guardian*. http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

Madden, M., & Rainie, L. (2015). Americans' Attitudes About Privacy, Security and Surveillance. https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Madison, J. (1792). Fourth Amendment — Browse — Constitution Annotated — Congress.gov — Library of Congress. https://constitution.congress.gov/browse/amendment-4/

Maggetti, M. (2010). Legitimacy and Accountability of Independent Regulatory Agencies: A Critical Review. https://ethz.ch/content/dam/ethz/special-interest/gess/cis/cis-dam/CIS_DAM_2015/WorkingPapers/Living_Reviews_Democracy/Maggetti.pdf

Manancourt, V. (2021). EU privacy law's chief architect calls for its overhaul. https://www.politico.eu/article/eu-privacy-laws-chief-architect-calls-for-its-overhaul/

Marx, G. T. (2015). Surveillance Studies. In *International Encyclopedia of the Social & Behavioral Sciences* (pp. 733–741). Elsevier. doi: 10.1016/B978-0-08-097086-8.64025-4

Masse, E. (2021). *Three Years Under GDPR* (tech. rep.). Access Now. Retrieved December 21, 2021, from https://www.accessnow.org/cms/assets/uploads/2021/05/Three-Years-Under-GDPR-report.pdf

Masse, E. (2022). *Four Years Under The EU GDPR: How To Fix Its Enforcement* (tech. rep.). Retrieved May 19, 2023, from https://www.accessnow.org/wp-content/uploads/2022/07/GDPR-4-year-report-2022.pdf

McClain, C., Faverio, M., & Park, E. (2023). How Americans View Data Privacy. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Miglicco, G. (2018). GDPR is here and it is time to get serious. *Computer Fraud & Security*, *2018*(9), 9–12. doi: 10.1016/S1361-3723(18)30085-X

Mitnick, B. M. (1980). *The Political Economy of Regulation: Creating, Designing, and Removing Regulatory Forms*. Columbia University Press.

Morris, D. (2024). Duane Morris LLP - Duane Morris Class Action Review - 2024: A Comprehensive Analysis of Class Action Litigation. https://www.duanemorris.com/pressreleases/duane_morris_class_action_review_2024_comprehensive_review_class_action_litigation_0124.html

Muir, R. (2017). Is Facebook Really 'Connecting the World'? - ExchangeWire.com. https://www.exchangewire.com/blog/2017/02/06/facebook_connecting_the_world/

Murgia, M. (2020). Google moves UK user data to US to avert Brexit risks [Section: Google LLC]. *Financial Times*. https://www.ft.com/content/135e5b66-53fb-11ea-90ad-25e377c0ee1f

Narayanan, A., & Shmatikov, V. (2007). How To Break Anonymity of the Netflix Prize Dataset. *arXiv:cs/0610105*. http://arxiv.org/abs/cs/0610105

Nast, C. (2022). How GDPR Is Failing. *Wired UK*. https://www.wired.co.uk/article/gdpr-2022

National Audit Office. (2016). *Performance measurement by regulators* (tech. rep.). https://www.nao.org.uk/wp-content/uploads/2016/11/Performance-measurement-by-regulators.pdf

National Audit Office. (2021). Good practice guidance Principles of effective regulation. *Design*.

National People's Congress (NPC) of the People's Republic of China. (2021). Personal Information Protection Law of the People's Republic of China. https://personalinformationprotectionlaw.com/

Nations, U. (n.d.). Universal Declaration of Human Rights. Retrieved February 3, 2024, from https://www.un.org/en/about-us/universal-declaration-of-human-rights

Nissenbaum, H. (2004). Privacy as Contextual Integrity Symposium - Technology, Values, and the Justice System. *Washington Law Review*, *79*(1), 119–158. https://heinonline.org/HOL/P?h=hein.journals/washlr79&i=129

Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. In *Privacy in Context*. Stanford University Press. doi: 10.1515/9780804772891

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48. doi: 10.1162/DAED_a_00113

NIST. (2008). NIST personal data - Glossary — CSRC. https://csrc.nist.gov/glossary/term/personal_data

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. doi: 10.1145/3313831.3376321

noyb. (2022). Data Protection Day: 41 Years of "Compliance on Paper"?! https://noyb.eu/en/data-protection-day-41-years-compliance-paper

noyb. (2023a). GDPRhub. https://gdprhub.eu/index.php?title=Welcome_to_GDPRhub

noyb. (2023b). Ireland: Corrupt GDPR procedures now "confidential". Retrieved July 3, 2023, from https://noyb.eu/en/ireland-corrupt-gdpr-procedures-now-confidential

noyb. (2023c). European Commission gives EU-US data transfers third round at CJEU. https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu

noyb. (2024). GDPR: A culture of non-compliance? https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance_2.pdf

O'Brien, R. (2016). Privacy and security: The new European data protection regulation and it's data breach notification requirements. *Business Information Review*, *33*(2), 81–84. doi: 10.1177/0266382116650297

OECD. (2011). *Setting the scene: The importance of regulatory policy* (tech. rep.). OECD. Paris. doi: 10.1787/9789264116573-4-en

OECD. (2019). Regulatory-effectiveness-in-the-era-of-digitalisation.pdf. https://www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf

OECD. (2022). Entrepreneurship - Enterprises by business size. http://data.oecd.org/entrepreneur/enterprises-by-business-size.htm

Ogus, A. (2004). *Comparing regulatory systems: Institutions, processes and legal forms in industrialised countries*. Edward Elgar Publishing. https://www.elgaronline.com/display/9781843764823.00016.xml

Ogus, A. I. (2004). *Regulation: Legal Form and Economic Theory*. Bloomsbury Publishing.

Oireachtas, H. o. t. (2023). Courts and Civil Law (Miscellaneous Provisions) Bill 2022: From the Seanad – Dáil éireann (33rd Dáil) – Wednesday, 28 Jun 2023 – Houses of the Oireachtas [Type: text]. https://www.oireachtas.ie/en/debates/debate/dail/2023-06-28/26

Orrick. (2021). China's New Data Security Law: What International Companies Need to Know. https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know

Oxford Analytica. (2019). Europe's national regulators hold key to GDPR success. *Emerald Expert Briefings*, *oxan-db*. doi: 10.1108/OXAN-DB243916

Parikh, T. (2024). Erik Brynjolfsson: 'This could be the best decade in history — or the worst' [Section: Artificial intelligence]. *Financial Times*. https://www.ft.com/content/b71759fe-397b-4688-bc81-b082edb25f31

Parliament, E. (2015). *The US legal system on data protection in the field of law enforcement* (tech. rep.). https://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf

Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press. doi: 10.4159/harvard.9780674736061

Pei, M. (2024). *The Sentinel State: Surveillance and the Survival of Dictatorship in China*. Harvard University Press.

Pelkmans, J., & Renda, A. (2014). Does EU Regulation Hinder or Stimulate Innovation? [Place: Rochester, NY Type: SSRN Scholarly Paper]. https://papers.ssrn.com/abstract=2528409

Peoples Republic of China. (2017). Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

Perry, R. (2019). GDPR – project or permanent reality? *Computer Fraud & Security*, *2019*(1), 9–11. doi: 10.1016/S1361-3723(19)30007-7

Politico. (2023). Deal over dim sum: China caves to EU on data to keep investors sweet. https://www.politico.eu/article/deal-over-dim-sum-china-caves-eu-data-keep-investors-sweet/

Politou, E., Alepis, E., & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4*(1). doi: 10.1093/cybsec/tyy001

Poritskiy, N., Oliveira, F., & Almeida, F. (2019a). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, *21*(5). doi: https://doi.org/10.1108/DPRG-05-2019-0039

Poritskiy, N., Oliveira, F., & Almeida, F. (2019b). The benefits and challenges of general data protection regulation for the information technology sector. *Digital Policy, Regulation and Governance*, *21*(5), 510–524. doi: 10.1108/DPRG-05-2019-0039

Posner, R. A. (1978). Economic Theory of Privacy. *Regulation*, *2*(3), 19–26. https://heinonline.org/HOL/P?h=hein.journals/rcatorbg2&i=131

Posner, R. A. (1981). The Economics of Privacy. *The American Economic Review*, *71*(2), 405–409. https://www.jstor.org/stable/1815754

Potoski, M., & Prakash, A. (2004). The Regulation Dilemma: Cooperation and Conflict in Environmental Governance. *Public Administration Review*, *64*(2), 152–163. doi: 10.1111/j.1540-6210.2004.00357.x

PR Newswire. (2019). GDPR One Year On: Survey Findings Show Consumer Awareness with Data Use is Concerningly Low: - A staggering eight percent of consumers globally feel they have a better understanding of how companies use their data since GDPR's introduction. Retrieved February 15, 2022, from http://www.proquest.com/central/docview/2229030700/citation/1A2AC7208F8D4253PQ/1

Prager, D. (2018). Google's New Slogan — RealClearPolitics. https://www.realclearpolitics.com/articles/2018/06/05/googles_new_slogan_137194.html

Prescott, K. (2024). Getting tough on AI could backfire on European Union [Section: business]. *The Times*. https://www.thetimes.co.uk/article/getting-tough-on-ai-could-backfire-on-european-union-p2dxr50zd

Presthus, W., & Sørum, H. (2019). Consumer perspectives on information privacy following the implementation of the GDPR. *JISPM - International Journal of Information Systems and Project Management*, (7), 19–34. doi: 10.12821/ijispm070302

Presthus, W., & Sørum, H. (2021). A three-year study of the GDPR and the consumer, 153–160. https://web.archive.org/web/20220206050656id_/http://www.iadisportal.org/components/com_booklibrary/ebooks/202103L019.pdf

Presthus, W., Sørum, H., & Andersen, L. R. (2018). GDPR Compliance in Norwegian Companies. *Proceedings from the Annual NOKOBIT Con-*

ference, *26*. Retrieved April 13, 2021, from https://ojs.bibsys.no/index.php/Nokobit/article/view/543

Prosser, W. L. (Ed.). (1960). Privacy. *California Law Review*. doi: 10.15779/Z383J3C

Rahnama, H., & Pentland, A. (2022). The New Rules of Data Privacy. *Harvard Business Review*. https://hbr.org/2022/02/the-new-rules-of-data-privacy

Ramirez, R., Mukherjee, M., Vezzoli, S., & Kramer, A. M. (2015). Scenarios as a scholarly methodology to produce "interesting research". *Futures*, *71*, 70–87. doi: 10.1016/j.futures.2015.06.006

Randall L. Calvert, Mathew D. McCubbins, & Barry R. Weingast. (1989). A Theory of Political Control and Agency Discretion. https://www.jstor.org/stable/2111064

Rattigan, K. M. (2025). 2024's Top Data Protection Settlements and Cybersecurity Changes. https://natlawreview.com/article/year-privacy-and-security-privacy-violations-large-scale-data-breaches-and-big

Reding, V. (2024). Keynote Speech by Viviane Reding — European Data Protection Supervisor. Retrieved July 16, 2024, from https://www.edps.europa.eu/press-publications/press-news/videos/keynote-speech-viviane-reding

Renieris, E. (2021). Why PETs (privacy-enhancing technologies) may not always be our friends. https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends/

Review, M. T. (2023). What are the hardest problems in tech we should be more focused on as a society? https://www.technologyreview.com/2023/11/01/1081939/big-questions-problem-solving-bill-gates-jennifer-doudna-lina-khan/

Richardson, V. J., Smith, R. E., & Watson, M. W. (2019). Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches. *Journal of Information Systems*, *33*(3), 227–265. doi: 10.2308/isys-52379

Rocher, L., Hendrickx, J., & Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, *10*. doi: 10.1038/s41467-019-10933-3

Rughinis, R., Rughinis, C., Vulpe, S. N., & Rosner, D. (2021). *From social netizens to data citizens: Variations of GDPR awareness in 28 European countries* (tech. rep. No. 109117). University Library of Munich, Germany. Retrieved February 15, 2022, from https://ideas.repec.org/p/pra/mprapa/109117.html

Ryan, G. W., & Bernard, H. R. (2003). Techniques to Identify Themes. *Field Methods*, *15*(1), 85–109. doi: 10.1177/1525822X02239569

Ryan, J. (2021). ICCL launches European Ombudsman complaint against European Commission's failure to take Ireland to court over the GDPR. https://www.iccl.ie/news/iccl-launches-european-ombudsman-complaint-against-european-commissions-failure-to-take-ireland-to-court-over-the-gdpr/

Ryan, J. (2023). Ryan to Reynders re UK adequacy. https://www.iccl.ie/wp-content/uploads/2023/05/Ryan-to-Reynders-re-UK-adequacy.pdf

Ryan, J., & Toner, A. (2020). *New data on GDPR enforcement agencies reveal why the GDPR is failing* (tech. rep.). Brave. Retrieved February 28, 2022, from https://brave.com/dpa-report-2020/

Sagacity. (2024). GDPR: The Good, the Bad, and the Future. https://widget.sitegpt.ai/c/369325253753569872

Salter, J. P. (2020). What does a level playing field mean? https://ukandeu.ac.uk/explainers/what-does-a-level-playing-field-mean/

Sanders, A. K. (2018). The GDPR One Year Later: Protecting Privacy or Preventing Access to Information Essays. *Tul. L. Rev.*, *93*(5), 1229–1254. Retrieved May 29, 2021, from https://heinonline.org/HOL/P?h=hein.journals/tulr93&i=1313

Sawers, P. (2023). Irish government criticized over proposed law-change that would 'muzzle' Big Tech critics. https://techcrunch.com/2023/06/26/ireland-big-tech-gdpr-dpc-critics/

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Schoeman, F. D. (1992). *Privacy and Social Freedom*. Cambridge University Press.

Scholz, J. T. (1984). Voluntary Compliance and Regulatory Enforcement. *Law & Policy*, *6*(4), 385–404. doi: 10.1111/j.1467-9930.1984.tb00334.x

Shyy, S. (2020). The GDPR's Lose-Lose Dilemma: Minimal Benefits to Data Privacy & Significant Burdens on Business. *U.C. Davis Bus. L.J.*, *20*(2), 137–164. Retrieved April 16, 2021, from https://heinonline.org/HOL/P?h=hein.journals/ucdbulj20&i=149

Skadden. (2021). China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies — Insights — Skadden, Arps, Slate, Meagher & Flom LLP. https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws

Skendžić, A., Kovačić, B., & Tijan, E. (2018). General data protection regulation — Protection of personal data in an organisation. *41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1370–1375. doi: 10.23919/MIPRO.2018.8400247

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2007). The affect heuristic. *European Journal of Operational Research*, *177*(3), 1333–1352. doi: 10.1016/j.ejor.2005.04.006

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564. doi: 10.2307/40041279

Solove, D. J. (2008). *Understanding Privacy* (SSRN Scholarly Paper No. ID 1127888). Social Science Research Network. Rochester, NY. https://papers.ssrn.com/abstract=1127888

Solove, D. J. (2020). The Three General Approaches to Privacy Regulation. https://teachprivacy.com/the-three-general-approaches-to-privacy-regulation/

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market. *Computers and Security*, *58*(100), 216–229. doi: 10.1016/j.cose.2015.12.006

Spence, D. B. (1997). Administrative Law and Agency Policy-Making: Rethinking the Positive Theory of Political Control. *Yale Journal on Regulation*,

14(2), 407–450. Retrieved March 23, 2023, from https://heinonline.org/HOL/P?h=hein.journals/yjor14&i=413

Spichtinger, D. (2024). New data protection and privacy laws have changed the regulatory landscape for researchers in the Global North [Type: LSE]. https://blogs.lse.ac.uk/impactofsocialsciences/2024/04/15/new-data-protection-and-privacy-laws-have-changed-the-regulatory-landscape-for-researchers-in-the-global-north/

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. *Proceedings of the 3rd ACM conference on Electronic Commerce*, 38–47. doi: 10.1145/501158.501163

Stanley, M. (2019). Understanding Regulation - The Organisational Behaviour of Regulators. https://www.regulation.org.uk/ob-regulators_behaviour.html

Sterling, G. (2010). Privacy, "The Creepy Line" And Beyond: It's Not Just About Google. https://searchengineland.com/privacy-the-creepy-line-and-beyond-its-not-just-about-google-52563

Strycharz, J., Ausloos, J., & Helberger, N. (2020). Data Protection or Data Frustration? Individual Perceptions and Attitudes towards the GDPR. *European Data Protection Law Review (EDPL)*, *6*(3), 407–421. Retrieved February 15, 2022, from https://heinonline.org/HOL/P?h=hein.journals/edpl6&i=436

Stutzman, F., Vitak, J., Ellison, N., Gray, R., & Lampe, C. (2012). Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook. *Proceedings of the International AAAI Conference on Web and Social Media*, *6*(1), 330–337. https://ojs.aaai.org/index.php/ICWSM/article/view/14268

Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). Unlocking the privacy paradox: Do cognitive heuristics hold the key? *CHI '13 Extended Abstracts on Human Factors in Computing Systems*, 811–816. doi: 10.1145/2468356.2468501

Tallberg, J. (2002). Paths to Compliance: Enforcement, Management, and the European Union. *International Organization*, *56*(3), 609–643. doi: 10.1162/002081802760199908

Tene, O., & Polonetsky, J. (2012). Big Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, *11*(5), [xxvii]–274. https://heinonline.org/HOL/P?h=hein.journals/nwteintp11&i=268

The Environment Agency. (2011). *Effectiveness of Regulation: Literature Review and Analysis* (tech. rep.). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/290502/scho0911bubh-e-e.pdf

The Information Commissioners Office. (2022). ICO Annual report 2021-2022. https://ico.org.uk/media/about-the-ico/documents/4021039/ico-annual-report-2021-22.pdf

The Irish Data Protection Commission. (2022). *Data Protection Commission AR 2021* (tech. rep.). Retrieved March 23, 2023, from https://www.dataprotection.ie/sites/default/files/uploads/2022-02/Data%20Protection%20Commision%20AR%202021%20English%20FINAL_0.pdf

Thierer, A. D. (2014). Privacy Law's Precautionary Principle Problem. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2449308

Thomas, D. R. (2006). A General Inductive Approach for Analyzing Qualitative Evaluation Data. *American Journal of Evaluation*, *27*(2). doi: 10.1177/1098214005283748

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134–153. doi: 10.1016/j.clsr.2017.05.015

Translate, C. L. (2021). Data Security Law of the PRC. Retrieved February 4, 2024, from https://www.chinalawtranslate.com/datasecuritylaw/

Tuta, H. (2020). UK Gmail users to lose EU data protection. https://tuta.com/blog/posts/uk-gmail-users-lose-eu-data-protection

United Nations. (1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

University, G. (2024). Fleshing out St Augustine. https://faculty.georgetown.edu/jod/texts/sundayheraldreview.html

US Department of Justice. (n.d.). The Foreign Intelligence Surveillance Act of 1978 (FISA) — Bureau of Justice Assistance. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286

US Supreme Court. (1965). Estelle T. Griswold et al. Appellants, v. State of Connecticut. https://www.law.cornell.edu/supremecourt/text/381/479

van der Marel, E., Bauer, M., Lee-Makiyama, H., & Verschelde, B. (2016). A methodology to estimate the costs of data regulations. *International Economics*, (146), 12–39. doi: 10.1016/j.inteco.2015.11.001

Véliz, C. (2021). *Privacy is Power*. Penguin. Retrieved July 15, 2024, from https://www.penguin.co.uk/books/442343/privacy-is-power-by-carissa-veliz/9780552177719

Venkataramakrishnan, S. (2021). GDPR fines jump as EU regulators raise pressure on business. *Financial Times*. Retrieved November 25, 2021, from https://www.ft.com/content/20b9430e-9058-4d7f-b953-d5d178def3c5

Vickery, A. (2008). An Englishman's Home Is His Castle? Thresholds, Boundaries and Privacies in the Eighteenth-Century London House*. *Past & Present*, *199*(1), 147–173. doi: 10.1093/pastj/gtn006

Vogel, D. (2009). *Trading Up: Consumer and Environmental Regulation in a Global Economy*. Harvard University Press.

Volpicelli, G. (2024). France means business with Mistral-Microsoft deal. https://www.politico.eu/article/why-france-chose-to-be-europes-ai-playground/

Voss, A. (2021). Fixing the GDPE: Towards Version 2.0. https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf

Voss, W. G., & Bouthinon-Dumas, H. (2021). *EU General Data Protection Regulation Sanctions in Theory and in Practice* (SSRN Scholarly Paper No. ID 3695473). Social Science Research Network. Rochester, NY. Retrieved February 17, 2022, from https://papers.ssrn.com/abstract=3695473

Wachter, S., Mittelstadt, B., & Russell, C. (2020). Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law

and AI [Place: Rochester, NY Type: SSRN Scholarly Paper]. doi: 10.2139/ssrn.3547922

Wallace, N., & Castro, D. (2018). *The Impact of the EU's New Data Protection Regulation on AI*. Centre for Data Innovation. Retrieved May 29, 2021, from https://datainnovation.org/2018/03/the-impact-of-the-eus-new-data-protection-regulation-on-ai/

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems*, *15*(3), 320–330. doi: 10.1057/palgrave.ejis.3000589

Warren, S. D., & Brandeis, L. D. (1890). Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://heinonline.org/HOL/P?h=hein.journals/hlr4&i=205

West, S. M. (2019). Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*, *58*(1), 20–41. doi: 10.1177/0007650317718185

White, S. (2018). General data protection regulation and the trust of the consumer [newspaper]. Retrieved January 10, 2021, from https://gdpr.report/news/2018/01/23/general-data-protection-regulation-trust-consumer/

Wikipedia. (2022). Goldilocks principle [Page Version ID: 1120728290]. Retrieved February 15, 2023, from https://en.wikipedia.org/w/index.php?title=Goldilocks_principle&oldid=1120728290

Wikipedia. (2024a). Regulatory technology. https://en.wikipedia.org/w/index.php?title=Regulatory_technology&oldid=1167034194

Wikipedia. (2024b). Big Tech. https://en.wikipedia.org/w/index.php?title=Big_Tech&oldid=1200526962

Wikipedia. (2024c). Pegasus (spyware). https://en.wikipedia.org/w/index.php?title=Pegasus_(spyware)&oldid=1210945241

William Bernhard. (1998). A Political Explanation of Variations in Central Bank Independence — American Political Science Review — Cambridge Core. https://www.cambridge.org/core/journals/american-political-science-review/article/political-explanation-of-variations-in-central-bank-independence/DAE8837A0A6FC400EE483BF9392E868C

Williams, M., & Moser, T. (2019). The Art of Coding and Thematic Exploration in Qualitative Research. *International Management Review*, *15*(1), 45–55, 71–72. Retrieved April 11, 2023, from https://www.proquest.com/docview/2210886420/abstract/E00F3EF3D7CD4724PQ/1

Williamson, D., Lynch-Wood, G., & Ramsay, J. (2006). Drivers of Environmental Behaviour in Manufacturing SMEs and the Implications for CSR. *Journal of Business Ethics*, *67*(3), 317–330. doi: 10.1007/s10551-006-9187-1

Wodi, A. (2023). The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review. *SSRN Electronic Journal*. doi: 10.2139/ssrn.4601142

Wodinsky, S. (2022). The Hidden Failure of the World's Biggest Privacy Law. https://gizmodo.com/gdpr-iab-europe-privacy-consent-ad-tech-online-advertis-1848469604

Wolff, J., & Atallah, N. (2020). Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020. doi: 10.2139/ssrn.3748837

Woods, D. W., & Ceross, A. (2022). Blessed Are The Lawyers, For They Shall Inherit Cybersecurity. *Proceedings of the 2021 New Security Paradigms Workshop*, 1–12. doi: 10.1145/3498891.3501257

World Economic Forum. (2020). Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators. https://www.weforum.org/pages/agile-regulation-for-the-fourth-industrial-revolution-a-toolkit-for-regulators/

Worledge, M., & Bamford, M. (2021). *Information Rights Strategic Plan: Trust and Confidence* (Commissioned Report). Information Commissioners Office. https://ico.org.uk/media/about-the-ico/documents/2620165/ico-trust-and-confidence-report-290621.pdf

Xu, H., Luo, X., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems*, *51*(1), 42–52. doi: 10.1016/j.dss.2010.11.017

Yale School of the Environment. (2024). As Use of A.I. Soars, So Does the Energy and Water It Requires. https://e360.yale.edu/features/artificial-intelligence-climate-energy-emissions

Zenner, K. (2021). Fixing the GDPR: Towards Version 2.0. Retrieved April 10, 2024, from https://www.kaizenner.eu/post/gdpr_vol2

Zhang, J., Hassandoust, F., & Williams, J. (2020). Online Customer Trust in the Context of the General Data Protection Regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems*, *12*(1). doi: 10.17705/1pais.12104

Zhu, K. Z., Julie, & Leng, C. (2020). How billionaire Jack Ma fell to earth and took Ant's mega IPO with him [Section: Asia Pacific]. *Reuters*. https://www.reuters.com/article/idUSKBN27L2GW/

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. doi: 10.1057/jit.2015.5

Zuboff, S. (2019a). *The Age of Surveillance Capitalism*. Public Affairs. Retrieved February 21, 2024, from https://www.hachettebookgroup.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/?lens=publicaffairs

Zuboff, S. (2019b). Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum*, *28*(1), 10–29. doi: 10.1177/1095796018819461

Appendix A

Interview Framework

The following text is the aide mémoire used when conducting structured face-to-face interviews with business executives on the impacts of the GDPR to their organisations, as described in Chapter 4.

Remind and reassure the interviewees that the conversation will abide by the university's ethics code and their contributions will be anonymized. Check they are comfortable with being recorded.

Part 1 Open questions

- Tell me about your job
- Industry sector & Size of company?
- What is your role, your title, your department?
- What does your company / department use customer data for? Describe

Part 2 Open questions

- Are you familiar with GDPR?
- How has it affected your day-to-day work / department / division / company?
- Biggest benefits?
- Biggest challenges?

Part 3 Raise topic areas if they haven't come up in answer to open questions. The benefits checklist is drawn from the academic literature review.

- Company's brand / reputation? Rationale?
- Customer trust level? How do you know?
- Legal certainty? Grey areas?
- Level playing field across Europe; Access to a bigger market for your company?
- GDPR compliance and competitive advantage in EU and in non-EU markets?
- Innovation? Have you seen new products / services?
- GDPR-led growth? Give examples. Investment incentive?
- Advertising? Changes post-GDPR? Targeting?
- GDPR-linked upgrades to internal systems and / or streamlined processes? Examples?

  - Security now versus before?

Part 4 Raise topic areas if they haven't come up in answer to open questions. The challenges checklist is drawn from the academic literature review.

  - Departmental impacts?
  - Company-wide and / or market impacts?
  - Compliance cost overheads?
  - Data audit impacts?
  - Data minimization impacts?
  - Data security rigidities?
  - Data breaches / Greater liabilities to fines?
  - Accountability and governance - how does it work?
  - Privacy rights - satisfying SAR's, right to correction and deletion?
  - Impact of privacy-first processes on advertising / marketing / servicing customers?

Part 5 Open questions about the future of GDPR

  - What makes good GDPR good?
  - Any recommendation about how to improve it?
  - What would the company be doing different today with data if GDPR did not exist?

Appendix B

Perceptions Survey

B.1 Tables of survey responses

Table B.1: Organisation size compared with division

	Customer Service	Finance	General management	Human resources	Information Technology	Legal/ Risk/ Compliance	Marketing/ Product Manager/ Digital Marketer	Operations/ Manufacturing	Sales/ Business Development	Sum
Micro 1–9	0	1	1	0	0	0	0	2	2	6
Small 10–49	3	1	2	0	2	0	0	1	2	11
Medium 50–249	2	0	3	0	2	1	3	7	1	19
Large 250–2,499	5	1	3	1	3	1	0	5	1	20
Very Large 2,500+	15	3	6	0	7	1	0	11	3	46
Sum	25	6	15	1	14	3	3	26	9	102

Table B.2: Perceived main purpose of the GDPR regulator.

Topics	Count	%
Monitor compliance	59	57.8%
Protect data	32	31.4%
Fine	11	10.8%
Misuse	11	10.8%
Don't know	8	7.8%
Investigate breaches	8	7.8%
Support consumers	8	7.8%
Support companies	7	6.9%
Take action	7	6.9%
Uphold consumer rights	6	5.9%
Protect people	5	4.9%
Ensure accuracy	3	2.9%
Audit	2	2.0%
Deal with complaints	2	2.0%
Enable individual to control personal data	2	2.0%
Impartial	2	2.0%
Transparency	2	2.0%
Can make SAR	1	1.0%
EU wide standard	1	1.0%
It is a con	1	1.0%
Promote data privacy	1	1.0%

Table B.3: Codes and frequency of advantages of the GDPR to the respondents' company

Topics	Count	%
Don't know	25	24.5%
Better care handling data	12	11.8%
Better personal data security	12	11.8%
Better data security	11	10.8%
Clear guidance	7	6.9%
Trust signal to employee	7	6.9%
Employee peace of mind	6	5.9%
Better data management	5	4.9%
Enforces compliance	5	4.9%
Trust signal to consumer	5	4.9%
Collect less data	4	3.9%
More transparency	4	3.9%
More awareness of penalties	3	2.9%
No advantage to company	3	2.9%
Training	3	2.9%
Employee privacy awareness	2	2.0%
More training	2	2.0%
More trust	2	2.0%
Reason to refuse	2	2.0%
Accountability	1	1.0%
Employee control over own data	1	1.0%
GDPR support industry	1	1.0%
More up to date	1	1.0%
Protects company	1	1.0%
Protects consumer	1	1.0%
Reassurance	1	1.0%
Tailored advertising	1	1.0%
Uniform training	1	1.0%

Table B.4: Perceived response by the participant's employer to the GDPR.

Main Questions	Strongly disagree	Disagree	Mildly disagree	Neither agree or disagree	Mildly agree	Agree	Strongly agree
GDPR has changed how I do my job at work	4.9%	9.8%	7.8%	14.7%	26.5%	28.4%	7.8%
I have not been put on GDPR-related privacy and cybersecurity training courses at work	23.5%	20.6%	9.8%	3.9%	6.9%	17.6%	17.6%
I've noticed new and/or widened roles and responsibilities at work that were inspired by GDPR	6.9%	11.8%	6.9%	16.7%	28.4%	24.5%	4.9%
I've noticed no new privacy and security software at work since GDPR	13.7%	27.5%	19.6%	11.8%	6.9%	14.7%	5.9%
I've noticed my employer has not changed their behaviour when handling personal customer data since GDPR	22.5%	32.4%	16.7%	13.7%	5.9%	4.9%	3.9%
My employer has not communicated to staff that it could face big fines for data misuse or data breaches under GDPR.	30.4%	26.5%	13.7%	7.8%	2.0%	13.7%	5.9%
My company is more transparent about how it uses customer data than before	3.9%	5.9%	4.9%	23.5%	30.4%	23.5%	7.8%
My company takes more care when handling personal data than before	2.0%	2.9%	2.9%	20.6%	18.6%	37.3%	15.7%
My company collects less personal data than before	4.9%	13.7%	9.8%	44.1%	9.8%	15.7%	2.0%
My company has not made material changes since GDPR	14.7%	31.4%	16.7%	19.6%	7.8%	3.9%	5.9%

Table B.5: Codes and frequency of disadvantages of the GDPR to the respondents company.

Topics	Count	%
Bureaucracy	23	22.5%
More processes	18	17.6%
Time-consuming	16	15.7%
No disadvantage	14	13.7%
Don't know	11	10.8%
No change	7	6.9%
Risk uncertain	7	6.9%
Extra costs	6	5.9%
Hinders marketing	6	5.9%
Limitation of use	6	5.9%
None	6	5.9%
Business development drawback	5	4.9%
More security	5	4.9%
Hinders customer service	4	3.9%
More workload	4	3.9%
Training	4	3.9%
Abuse of rights	3	2.9%
Answering SARs	2	2.0%
Staff resistence	2	2.0%
More careful handling	1	1.0%
Prefer to ignore GDPR and pay fine	1	1.0%

B.2 Regression analysis

Table B.6: Linear Models for outcome variables associated with the organisation. The rows are the independent variables, which were selected stepwise in a cross-validated manner to minimize model error.

Dependent / Independent	Not scared & do bare minimum	Scared & changed behaviour	Not scared because fines unlikely	More hassle than worth	Good for my company	Knowledge of compliance	Knowledge of obligations	Observed changes
Consumer feels privacy is better	-0.269*** (0.093)		-0.391*** (0.090)	-0.371*** (0.106)	0.664*** (0.074)			
Awareness of ICO at work	-0.211** (0.091)							0.190** (0.081)
Knowledge of compliance							0.273*** (0.090)	0.221*** (0.083)
Knowledge of GDPR						0.648*** (0.063)		
Knowledge of rights					-0.186** (0.074)		0.324*** (0.090)	
Knowledge of obligations								0.154** (0.071)
Knowledge of Roles of Regulator				0.173** (0.080)				
Negative impacts				0.231*** (0.077)				0.254*** (0.069)
Positive impacts		0.399*** (0.091)		-0.338*** (0.100)				0.310*** (0.077)
Changes in company behaviour						0.298*** (0.063)		
Participant certainty	0.253*** (0.089)		0.197** (0.090)					-0.170** (0.069)
R-squared	0.268	0.159	0.227	0.451	0.451	0.662	0.195	0.570
R-squared Adj.	0.246	0.151	0.212	0.429	0.440	0.655	0.179	0.543

Table B.7: Linear Model for outcome variables associated with the individual.

Dependent / Independent	More hassle than worth it	Consumer feels privacy is better	On balance, GDPR is worth it
Consumer feels privacy is better	-0.602*** (0.074)		0.829*** (0.056)
Knowledge of GDPR		0.220*** (0.072)	
Knowledge of Roles of Regulator		0.232*** (0.069)	
Negative impacts	0.233*** (0.074)	-0.205*** (0.069)	
Positive impacts		0.551*** (0.072)	
R-squared	0.459	0.547	0.687
R-squared Adj.	0.448	0.528	0.684

B.3 Survey content

Prolific ID

What is your Prolific ID?
Please note that this response should auto-fill with the correct ID

${e://Field/PROLIFIC_PID}

Consent & Employment Tenure Block

This survey is part of a study being conducted at University College London. We are asking people a range of questions about privacy in the online age. Your participation in this study is completely voluntary; choosing not to take part will not disadvantage you in any way. If you do decide to take part, you are still free to withdraw at any time and without giving a reason. You will receive full payment only upon completing the study.

Please be aware we have attention checks and nonsense checks in some questions, and we reserve the right not to pay if we feel the respondent has raced through the questions unthinkingly.

The survey is entirely anonymous, and we will not collect any personal data from you. The anonymous survey responses may be shared with other researchers and appear in academic publications. You may contact us if you have additional questions at gerard.buckley.18@ucl.ac.uk or through prolific. If you want to raise a complaint, please contact Dr Ingolf Becker (i.becker@ucl.ac.uk). If you feel your complaint has not been handled to your satisfaction, you can contact the Chair of the Security and Crime Science Research Ethics Committee at scs.ethics@ucl.ac.uk. This research project has been approved by the ethics committee in the Department of Security and Crime Science at UCL. You can check how far you have progressed in the survey by looking at the bar at the top of the screen.

By clicking "Yes," I confirm the following: I am 18 years or older I understand and agree to all the information listed above

- ○ Yes
- ○ No

How long have you worked for your current organisation?

- ○ Under 5 years
- ○ More than 5 years

Company & Departmental Details & GDPR Familiarity Test Block

Roughly how many people work in your organisation

- ○ Micro 1-9
- ○ Small 10-49
- ○ Medium 50-249
- ○ Large 250-2,499
- ○ Very Large 2,500+

What department do you work in?

- ○ Legal/Risk/Compliance
- ○ Finance
- ○ General management
- ○ Customer Service
- ○ Sales/Business Development
- ○ Information Technology
- ○ Human resources
- ○ Marketing/Product Manager/Digital Marketer
- ○ Operations/Manufacturing

Have you heard of GDPR or The General Data Protection Regulation before now?

- ○ Yes
- ○ No

Sad Farewell to GDPR No-Knows Block

Sadly your answer makes the rest of the questionnaire redundant. Please click through so that we register your work for payment.

Awareness of Consumer Rights & Employer Obligations Block

How well do you know the rights you get as a consumer under GDPR?
Use the slider to show your level of knowledge where 0 = I know nothing and 100 = I am a data privacy expert

0 10 20 30 40 50 60 70 80 90 100

0 10 20 30 40 50 60 70 80 90 100

Knowledge

Which of the following are consumer rights regarding personal data under GDPR?

	Yes	No	Unsure
Right to be informed about collection and use of your data	○	○	○
Ability to delete your data, also known as the "right to be forgotten"	○	○	○
Ability to rectify inaccurate or incomplete data	○	○	○
Ability to access and receive a copy of your data	○	○	○
Right to collect share of financial penalty if company has been fined for a data breach	○	○	○
Right to collect micro-payment for your data	○	○	○
Ability to swim across the channel	○	○	○
Right to check your attention by clicking yes	○	○	○

How well do you know what your company has to do in order to comply with GDPR?
Use the slider to show the degree of your knowledge where 0 = I know nothing and 100 = I am an expert

Strongly disagree | Somewhat disagree | Neither agree nor disagree | Somewhat agree | Strongly agree

0 10 20 30 40 50 60 70 80 90 100

Knowledgeable

Which of the following are rules that a company must comply with when handling personal data under GDPR?

	Yes	No	Unsure
Fair, lawful and transparent use only	○	○	○
Specific and explicit purpose	○	○	○
Data can be kept for longer than necessary	○	○	○
Limited to only what is necessary and relevant	○	○	○
Must be made available to national security if asked	○	○	○
Data must be kept safe and secure	○	○	○
Data must be kept up to date	○	○	○

Consumer Regulator Awareness Block

What is the name of the GDPR regulator in the UK?

- ○ The Data Protection Agency (DPA)
- ○ The Data Protection Authority (DPA)
- ○ The Office of Data (OfDat)
- ○ The British Privacy Authority (BPA)
- ○ The Information Commissioners Office (ICO)

What is/are the main purpose(s) of the GDPR regulator? (The answer is not just 'to regulate'!)

Which of the following roles is the regulator supposed to do?

	Yes	No	Unsure
Fine companies for proven data misuse	☐	☐	☐
Deal with concerns/complaints raised by members of the public	☐	☐	☐
Fine companies for data breaches	☐	☐	☐
Give out kittens for Christmas	☐	☐	☐
Give advice to members of the public	☐	☐	☐
Give guidance to companies about their obligations	☐	☐	☐
Maintain a public register of data controllers	☐	☐	☐

Have you heard of companies being fined by the regulator?

- ○ Yes
- ○ No

If so, can you remember the companies names?

Company Changes Block

To what extent do you agree with the following statements about how your company has responded to GDPR

	Strongly agree	Agree	Mildly agree	Neither agree nor disagree	Mildly disagree	Disagree	Strongly disagree
GDPR has changed how I do my job at work	○	○	○	○	○	○	○
I have not been put on GDPR-related privacy and cybersecurity training courses at work	○	○	○	○	○	○	○
I've noticed new and/or widened roles and responsibilities at work that were inspired by GDPR	○	○	○	○	○	○	○
I've noticed no new privacy and security software at work since GDPR	○	○	○	○	○	○	○
I've noticed my employer has not changed their behaviour when handling personal customer data since GDPR	○	○	○	○	○	○	○
My employer has not communicated to staff that it could face big fines for data misuse or data breaches under GDPR.	○	○	○	○	○	○	○
My company is more transparent about how it uses customer data than before	○	○	○	○	○	○	○
My company takes more care when handling personal data than before	○	○	○	○	○	○	○
My company collects less personal data than before	○	○	○	○	○	○	○
My company has not made material changes since GDPR	○	○	○	○	○	○	○
I've noticed the attention check and I select strongly disagree	○	○	○	○	○	○	○

Employee Regulator Awareness Block

Have you heard of the Information Commissioners Office or ICO before now?

○ Yes
○ No

For your information, the ICO is the name of the GDPR regulator in the UK

○ Please click

Please indicate the strength of your agreement with the following statements about the ICO

	Strongly Agree	Agree	Mildly Agree	Neither agree nor disagree	Mildly Disagree	Disagree	Strongly Disagree
The ICO does pop up occasionally in discussions at work	○	○	○	○	○	○	○
Staff have been informed that the company could face big fines by the ICO for data misuse or data breaches	○	○	○	○	○	○	○
In work discussions, the ICO is well regarded	○	○	○	○	○	○	○

Benefits & Challenges to Company

Please indicate the strength of your feeling regarding the following statement

	Strongly agree	Agree	Mildly agree	Neither agree nor disagree	Mildly disagree	Disagree	Strongly disagree
The requirements of GDPR have made my job harder and/or more cumbersome	○	○	○	○	○	○	○

What have you observed to be the biggest disadvantage of GDPR to your company?

What have you observed to the biggest advantage of GDPR to your company?

To what extent would you agree with the following statements about the impact of GDPR on your company?

	Strongly Agree	Agree	Mildly Agree	Neither agree or disagree	Mildly Disagree	Disagree	Strongly Disagree
Receive more freedom of information requests	○	○	○	○	○	○	○
More compliance costs	○	○	○	○	○	○	○
More cyber-security costs	○	○	○	○	○	○	○
Better data security	○	○	○	○	○	○	○
Less bureaucracy	○	○	○	○	○	○	○
Better ability to pay attention and select 'agree' here	○	○	○	○	○	○	○
Better awareness of the importance of data privacy practices	○	○	○	○	○	○	○
Less up-to-date customer databases	○	○	○	○	○	○	○
Better trust and confidence in the company brand	○	○	○	○	○	○	○

The Key Question

To what extent would you agree to the following statements about GDPR

	Strongly Agree	Agree	Mildly Disagree	Neither agree nor disagree	Mildly Disagree	Disagree
GDPR means makes me feel more in control of personal my data	○	○	○	○	○	○
GDPR is good for my company	○	○	○	○	○	○
On balance, GDPR is worth it	○	○	○	○	○	○
GDPR is good for the consumer	○	○	○	○	○	○

Last question - To what extent do you agree with these statements?

	Strongly Agree	Agree	Mildly Disagree	Neither agree or disagree	Mildly Disagree	Disagree	Strongly Disagree
GDPR is more hassle than it is worth to me as a consumer	○	○	○	○	○	○	○
Companies are not scared by GDPR and do the bare minimum to comply	○	○	○	○	○	○	○
Companies are scared by GDPR and really have changed their behaviour	○	○	○	○	○	○	○
Companies are not scared by GDPR because they know the probability of being fined is low	○	○	○	○	○	○	○
GDPR is more hassle than it is worth to my company	○	○	○	○	○	○	○
GDPR has improved privacy	○	○	○	○	○	○	○

Farewell & Get Paid

Thank you for your time taking this survey.
Please click the button to be redirected and register your submission.

Block 13

Powered by Qualtrics

Appendix C

Codebook

The following tables show the codebook grouped by theme.

Table C.1: Codes in the Cynical View theme

Appear to be in Control
Bad Manners to judge judges
Cases trump Investigations
Complexity of inconsistent systems
Cost Budget
Credibility of Regulator Authority
Cross Border cases are not that important
Decisions that stand up in Court
Duplicitous annual Reports
Fight it up to ECJ
Fines bad measure
Futile
Lack of central database
Lawyers act for plaintiffs
Never thought about it
Numbers only tell half the story
Perceptions are not enough
Scrutiny by court
Scrutiny by Gov
Success =Low or No Breaches
Success =Low number of fines
Success =No spam no cold calls
Success =No fines
Terminology complexity
Transparency
Transparency of Annual Reports
CNIL v Spanish v Irish
Data is not safer
Rubbish DPA Reports
Rubbish EDPB Reports
Compliance Theatre
Organisational agenda
Outcomes v Resources
Personal agenda of staff
Procedural v Substantive
Secretive behaviour

Table C.2: Codes in the Lofty View theme

Accessible
Accountable
Appreciate value of data
Comparative benchmarks
Change Agents
Depends on Regulation Objectives
Leadership
Learning organisation
Metrics
View NGOs as helpers
Overall Compliance
Individual v corporate perspective
Proportionate
Reg Tech
Stakeholder Balance
Vision
A focus on fines is wrong
Global importance
Promote priority in companies
Spur to action
Behaviour change
Correct market failure
Create Trust
Individual Responsibility
Make the rules for everybody

Table C.3: Codes in the Enforcer theme

Business Support
Business Guidence
Not a balance of Equals
Enforcement
Fines: Punishment
Fines: Counterproductive
Fines: Go after parent company
Fines: Graded in severity
Fines: Public Relations
Fines: Can be a pro-business PR-weapon
Fines: Sanction power
Fines: Sin of commission v omission
Investigations
Media impact
Monitoring
Pace of decision making
Stop Order
Compliance with Regs & Rules
Drive-up Accountability Responsibility Integrity
Drive-up & maintain standards
Investigate Data Breaches
Reputational Impact
Useful Stick

Table C.4: Codes in the Protector theme

Complaint Handling
Educate
NGOs as assessors
Number of complaints
Number of Decisions
Number of DPOs in country
Number of opinions followed by Legislators
Powers Used metric
Success=Noyb Metrics
Consumer Individual Orientated
Educate
Public Awareness
Empowerment of the Consumer
Investigate Complaints
Protect Privacy

Table C.5: Codes in the Guide theme

Business Communications
Business Support & Guidence
Breach Reports are useful
Case studies are useful
Certainty
Collaborative
Credible Staff
Good website
Relationships with Business
Victim or Villain
Partner
Educate Business
Raise Awareness
Obfuscation
Poor Guidance

Table C.6: Interview Protocol

Participant information sheet check, Consent check, recording check.	
Double-check that the interviewee is familiar with the GDPR and has had some involvement with DPAs.	
RQ1	
1	What are the objectives of a GDPR privacy regulator?
2	You said the objectives were X, Y, and Z. Taking each in turn, what criteria do you use to judge their effectiveness in achieving those objectives?
RQ2	
Imagine you are doing a DPA's annual performance review.	
Here are 10 KPIs with which to evaluate them.	
3	What do you think of each KPI 1 to 10?
4	How would you rank the KPIs in terms of importance and why?
5	Would you amalgamate or drop some KPIs?
6	If you took off your (business/regulator) hat, would that change your opinion of their importance? Why?
7	Can you think of alternative KPIs?