Computer Law & Security Review 54 (2024) 106033

Contents lists available at ScienceDirect

Computer Law & Security Review: The International Journal of Technology Law and Practice

journal homepage: www.elsevier.com/locate/clsr

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

Gerard Buckley [a,*], Tristan Caulfield [a], Ingolf Becker [b]

[a] Department of Computer Science, University College London, Gower Street, WC1E 6BT, London, UK
[b] Department of Security & Crime Science, University College London, Gower Street, WC1E 6BT, London, UK

ARTICLE INFO

Keywords:
Privacy
Data protection
Regulation
Evolution
Future thinking
Scenarios

ABSTRACT

The digital age has made personal data more valuable and less private. This paper explores the future of the European Union's General Data Protection Regulation (GDPR) by imagining a range of challenging scenarios and how it might handle them. We analyse United States', Chinese and European approaches (self-regulation, state control, arms-length regulators) and identify four key drivers shaping the future regulatory landscape: econopolitics, enforcement capacity, societal trust, and speed of technological development. These scenarios lead us to envision six resultant versions of GDPR, ranging from laxer protection than now to models empowering individuals and regulators. While our analysis suggests a minor update to the status quo GDPR is the most likely outcome, we argue a more robust implementation is necessary. This would entail meaningful penalties for non-compliance, harmonised enforcement, a positive case to counter the regulation-stifles-innovation narrative, defence of cross-border data rights, and proactive guidelines to address emerging technologies. Strengthening the GDPR's effectiveness is crucial to ensure the digital age empowers individuals, not just information technology corporations and governments.

1. Introduction

As society grows ever more dependent on technology, concerns for our privacy intensify. Every time we interact online, we leave an electronic trail behind us that reveals more than we can imagine about our inner selves. Technology companies collect and process this data and resell it to other companies and state agencies. What the data is used for and whether it is beneficial or detrimental to our interests is often unknowable. This is why privacy and data protection regulation is essential.

Striking the right level of regulation is always a challenge. What the ideal balance is between the needs of society, business, or the state is an issue hotly debated from diverse philosophical, political and economic viewpoints. The answer to this question in Europe is the European Union (EU) General Data Protection Regulation (GDPR) [1]. Representing the other two large regulatory blocks, the United States (US) and China have come to different conclusions.

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 [2]. 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

* Corresponding author.
E-mail addresses: gerard.buckley.18@ucl.ac.uk (G. Buckley), t.caulfield@ucl.ac.uk (T. Caulfield), i.becker@ucl.ac.uk (I. Becker).

https://doi.org/10.1016/j.clsr.2024.106033

Available online 17 August 2024

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: Section 2 summarises the contestable definition of privacy, the function and form of regulation, and how these are expressed in privacy regulation. Section 3 constructs its analysis of the future in several stages, starting with structural forces and then condensing them into four key themes. Section 4 envisions six of 81 potential scenarios that shape six versions relative to GDPR V1.0. It discusses their plausibility and likely uptake. Section 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.

2. Background

In this section, we provide a brief background on the difficult-to-define notion of privacy, the theory of regulation and how these concepts are translated into privacy regulations in the EU, the US and China. The legal summaries focus on the GDPR and, to a lesser degree, the other two regimes.

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 2.3. 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 enshrined in law. By that time, 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' [3]. As technology advanced, privacy and the way it could be violated changed. In 1891, the American lawyers Samuel Warren and Louis Brandeis [4] 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 [5]. 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 [6] 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' [7,8]. Ferdinand Schoeman [9] expanded it to mean a system of norms that protect social freedoms and self-expression. Solove [10] 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 [11] 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 [7] 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 [12]. Multiple surveys by the Pew Research Centre [13,14] 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 [15].

In 2004, Nissenbaum [16,17] 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' [18]. 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' [19] has been known to information security professionals for some time, Professor Shoshana Zuboff [20] is widely credited for introducing the term 'surveillance capitalism' into mainstream discourse to describe this loss of control. In response, scholars like Brunton & Nissenbaum [21] propose obfuscation techniques to counter digital surveillance. Veliz [22] 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. [23] and Pasquale [24] tackle algorithm opacity, while Gasser [25] and Hartzog [26] 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. Regulation theory

Regulation theory is a vast field of study. We limit ourselves accordingly to a high-level understanding of its form and function and how that applies to privacy and data protection regulations.

According to the OECD, regulation is indispensable to the proper functioning of economies and societies [27] and is a key tool for governments to achieve policy objectives. A classic definition of regulation [28] 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'.

Governments regulate for many reasons. The technical justification for regulation is that it addresses market failures that are not in the public interest [29–31] (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 self-interest and the interests of society [32].

There are different 'types' of regulatory interventions. A simplified taxonomy by Pelkman and Renda [33] 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.

A significant distinction in regulatory approaches lies between principles-based regulations and rules-based regulations. 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, prioritising 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 businesses 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 [34]. 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 [35]. Notably, it reverses the burden of proof: the agent proposing the activity must prove the activity is not harmful.

In the US, Solove [36] classifies three high-level approaches to privacy law:

- 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: Organisations 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.

2.3. Applied privacy theory

Privacy is recognised as a universal human right by the United Nations, while data protection is not. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12) [37], the European Convention of Human Rights (Article 8) [38] and the European Charter of Fundamental Rights (Article 7) [39]. How this right is respected in practice varies.

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. In Europe, data protection is governed by Article 8 of the EU Charter of Fundamental Rights [40], the General Data Protection Regulation (GDPR) [1] and country-specific data protection acts such as the UK Data Protection Act 2018 [41]. Organisations have legal obligations with the processing of personal data, and individuals have rights, including information, access, rectification, objection and erasure. US laws do not protect personal data (known as Personally Identifiable Information (PII)) in such a wide manner [42]. 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. Chinese laws lean towards the EU model, but unlike the GDPR, the PIPL's definition of personal data does not include online identifiers, health, biometric, and genetic data, among other concepts [43].

The success of any regulation ultimately depends on how well it is executed. Recent research by Buckley et al. [44] has shown how difficult it can be to assess the performance of data protection regulators, even when they should be easily comparable in the case of the GDPR across the EU member states.

2.4. EU, US & Chinese privacy regulation

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 [45]. 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.

In the EU, the Data Protection Directive 1995 [46] was replaced with the GDPR in 2018 [1]. 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' [47]. 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 ceiling on maximum fines was raised to 4% of global turnover. It has achieved these aims to a limited extent. Research [48] shows that consumers are more aware of their rights, companies welcome a more uniform market, and the EU has made high-profile fines. Critics would argue that omnipresent privacy notices have

numbed consumers into giving away their data rights; businesses view compliance overheads as a regressive tax favouring larger companies and stifling innovation, and enforcement has been judged disappointing in some quarters. More broadly, critics fear that GDPR is too static and too easy to be outmanoeuvred by new technologies by Big Tech. Examples include AI, IoT and Big Data, which will be discussed in more detail in Section 3.5. (As an aside, Big Tech is the commonly used informal term that refers loosely to the most dominant information technology companies [49].)

For some critics, GDPR is not enough. For example, Members of the European Parliament (MEPs) published their own report [50] to shame Brussels for being too slow to tame Big Tech. They suggested a switch to a presumption of guilt so that Big Tech cannot take advantage of delays and dominate markets before cases come to court. They also suggested a significant increase in fines from 4% to 10% of global revenue to make the punishments more meaningful.

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). 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) [51], the Data Services Act (DSA) [52], the Data Act (DA) [53], the Artificial Intelligence Act (AIA) [54] and the ePrivacy Regulation [55]. 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.

In the US, no singular law covers all types of data privacy. Unlike Europe, US consumers, by and large, have had to rely on the Fourth Amendment. It 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' [56]. 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 [57,58].

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 [59] 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.

As with environmental regulation, the state of 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 regulation theory, the CCPA model leans more on consumers exercising their rights than documentation and governance compared to the GDPR.

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 monetise 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' [60]. Since her appointment in 2021, Ms 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.

In China, we see a third vastly different approach to privacy and antitrust in the digital economy. Emch [61] 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 [62]. 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 [63]. 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' [64], 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) [65,66] and the Personal Information Protection Law (PIPL) [67] provide more specificity about the data localisation, data export and data protection requirements than first appeared in the Chinese Cybersecurity Law in 2017 [68].

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) [69], 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 European Union's GDPR [70]. '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 anonymised is not covered [71]. 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.

2.5. Artificial intelligence act

The EU AI Act [72], 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 [50].

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.

2.6. Summary

While global consensus exists on the need for digital privacy protection, there is no singular agreed definition of privacy, and approaches differ. The US relies on market self-regulation, China trusts the state, and Europe employs arms-length regulators. The enforcement approaches also differ, with the US favouring notice and consent while China and Europe adopt more prescriptive measures. Next, we explore what will influence change in this regulatory landscape.

3. Analysis

In this section, driver mapping and the political, economic, societal, technological, legislative and environmental (PESTLE) [73] 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.

3.1. 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 enquiry is one way of generating interesting research [2]. The scenarios are not predictions. Rather, they represent a multi-dimensional potential future space.

The PESTLE analysis framework [73] 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', [73] 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 [74] and to support evidence-based policy decision-making [75,76].

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.

3.2. Geopolitical landscape

Geopolitics and data protection are tightly intertwined. In 'Global Governance Challenges' [77], Carr and Llanos describe three main approaches to governing data that currently coexist: a US 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 US 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.

The Chinese approach follows the US model of 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 US, 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 US approach must change to maintain its dominance in the data economy and 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 [77].

The 'California effect' was formulated by Vogel [78] 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' [79] 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' [80], 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 US 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 US and the EU best exemplifies this institutional and transboundary challenge. The latest deal, known as the EU-US Data Privacy Framework [81], 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 US intelligence agencies, exposed by Edward Snowden [82] 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 [83]. A pre-PIPL EU report [84] 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'. 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 [85].

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 US 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 US-EU link is the most trafficked at present, we will consider a range of end-states: US prevails, EU prevails, or both muddle along.

3.3. 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 US technology companies. Fines were deemed 'peanuts' or 'pocket money' relative to the size of the companies [86,87]. 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) [86].

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 [88,89]. 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 [90] confirms intuitively that fines focus the minds of business leaders and are how the general public perceives the virility of their regulator [91,92]. 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.

3.4. 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 [93]. 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 [94] 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 [95], 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' [96]. 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.

3.5. 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 [97]. 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 [98] 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 [99]. More recently in 2019, researchers published a method to correctly re-identify 99.98% of individuals in anonymised datasets with just 15 demographic attributes [100].

Some critics [101] 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' [102], 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 [103] (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.

3.6. 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.

4. Results

As summarised in Section 3.6, 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 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.

4.1. 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 Fig. 1, to show their relative positioning and summarised in Table 1. 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.

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 Fig. 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 but with the important caveat that it may compromise citizens' rights if it conflicts with the interests of chosen 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.

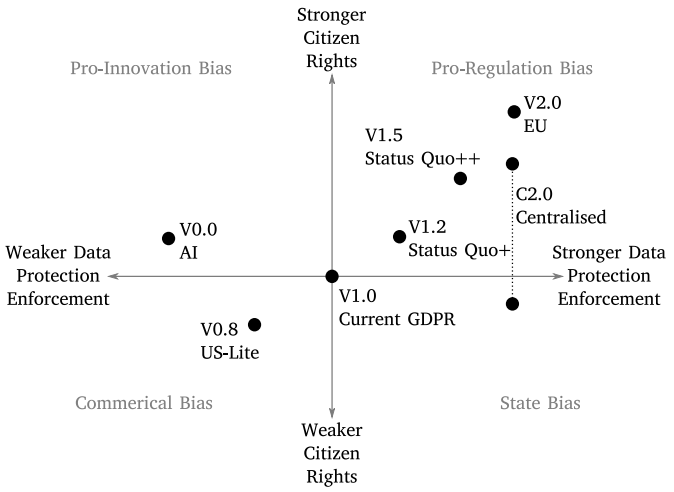

Fig. 1. Version Positioning.

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 [98].

Table 1 summarises the six scenarios in a version-dimension matrix. Next, we describe and critique the scenarios in more detail.

4.2. AI V0.0

This is the nightmare technology-driven scenario. Contrary to the optimistic 2020 AI Impact EP report [98], 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 [104]. Surveillance, data and shame become socially accepted behaviour modifiers [105]. Commercially, it assumes the pro-innovation narrative prevails, which blocks pre-emptive 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

Table 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

common sense prevails, and a new post-AI privacy norm becomes codified.

Some scholars [106] 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 [107]. A market analyst [108] 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.

4.3. 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. 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 [109]. 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) [110] 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 [111,112]. 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.

4.4. 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 Nyob complain that authorities fail to get businesses to comply properly.

4.5. 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 [113] 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 [114] and they may face stricter enforcement as there is a perception that regulators find it easier to handle smaller organisations than big multinationals [115]. 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' [116].

4.6. 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 [117] 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.

4.7. 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 misinformation. 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 Fig. 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 [118] and chilling innovation in AI over content restrictions [119]. Furthermore, some countries may be put off being identified with Chinese-style state control.

5. 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 € 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 [82] 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 [120], 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 [121], 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' [122].

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.

6. 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 utilises 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 enquiry.

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.

Funding and disclosure statement

Gerard Buckley is supported by UK EPSRC grant no. EP/S022503/1. Ingolf Becker is supported by UK EPSRC grant no. EP/W032368/1.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] EU. General data protection regulation (GDPR) – official legal text. 2018, URL https://gdpr-info.eu/,

[2] Ramirez Rafael, Mukherjee Malobi, Vezzoli Simona, Kramer Arnoldo Matus. Scenarios as a scholarly methodology to produce 'interesting research'. Futures 2015;71:70–87. http://dx.doi.org/10.1016/j.futures.2015.06.006.

[3] Vickery Amanda. An englishman's home is his castle? Thresholds, boundaries and privacies in the eighteenth-century London house*. Past Present 2008;199(1):147–73. http://dx.doi.org/10.1093/pastj/gtn006.

[4] Warren Samuel D, Brandeis Louis D. Right to privacy. Harv Law Rev 1890;4(5):193–220, URL https://heinonline.org/HOL/P?h=hein.journals/hlr4&i=205.

[5] United Nations. Universal Declaration of Human Rights, URL https://www.un.org/en/about-us/universal-declaration-of-human-rights, Publisher: United Nations.

[6] Prosser William L, editor. Privacy. California Law Rev 1960. http://dx.doi.org/10.15779/Z383J3C.

[7] Kumaraguru Ponnurangam, Cranor Lorrie. Privacy indexes: A survey of westin's studies. Technical report 856, Carnegie-Mellon University; 2005, URL http://repository.cmu.edu/isr/856.

[8] Davies Thomas. Recovering the original fourth amendment. Michigan Law Rev 1999;98(3):547–750, URL https://repository.law.umich.edu/mlr/vol98/iss3/2.

[9] Schoeman Ferdinand David. Privacy and social freedom. Cambridge University Press; 1992.

[10] Solove Daniel J. Understanding privacy. SSRN scholarly paper ID 1127888, Rochester, NY: Social Science Research Network; 2008, URL https://papers.ssrn.com/abstract=1127888.

[11] Gormley Ken. One hundred years of privacy. 1992, URL https://heinonline.org/HOL/Page?handle=hein.journals/wlr1992&div=57&g_sent=1&casa_token=&collection=journals.

[12] Ackerman Mark S, Cranor Lorrie Faith, Reagle Joseph. Privacy in e-commerce: examining user scenarios and privacy preferences. In: Proceedings of the 1st ACM conference on electronic commerce - EC '99. Denver, Colorado, United States: ACM Press; 1999, p. 1–8. http://dx.doi.org/10.1145/336992.336995.

[13] Auxier Brooke, Rainie Lee, Anderson Monica, Perrin Andrew, Kumar Madhu, Turner Erica. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. Pew Res Center: Internet Sci Tech 2019. URL https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[14] Madden Mary, Rainie Lee. Americans' attitudes about privacy, security and surveillance. Pew Res Center Internet Sci Tech 2015. URL https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[15] IPSOS. Internet users' trust in the Internet has dropped significantly since 2019 | Ipsos. 2022, URL https://www.ipsos.com/en/trust-in-the-internet-2022.

[16] Nissenbaum Helen. Privacy as contextual integrity symposium - technology, values, and the justice system. Washington Law Rev 2004;79(1):119–58, URL https://heinonline.org/HOL/P?h=hein.journals/washlr79&i=129.

[17] Nissenbaum Helen. A contextual approach to privacy online. Daedalus 2011;140(4):32–48. http://dx.doi.org/10.1162/DAED_a_00113.

[18] Koops Bert-Jaap, Newell Bryce Clayton, Timan Tjerk, Skorvanek Ivan, Chokrevski Tomislav, Galic Masa. A typology of privacy. Univ Pennsylvania J Int Law 2016;38(2):483–576, URL https://heinonline.org/HOL/P?h=hein.journals/upjiel38&i=489.

[19] Pei Minxin. The sentinel state: surveillance and the survival of dictatorship in China. Harvard University Press; 2024.

[20] Zuboff Shoshana. Surveillance capitalism and the challenge of collective action. New Labor Forum 2019;28(1):10–29. http://dx.doi.org/10.1177/1095796018819461, Publisher: SAGE Publications Inc.

[21] Brunton Finn, Nissenbaum Helen Fay. Obfuscation: A user's guide for privacy and protest. MIT Press; 2015, http://dx.doi.org/10.7551/mitpress/9780262029735.001.0001.

[22] Véliz Carissa. Privacy is power. Penguin; 2021, URL https://www.penguin.co.uk/books/442343/privacy-is-power-by-carissa-veliz/9780552177719.

[23] Wachter Sandra, Mittelstadt Brent, Russell Chris. Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. 2020, http://dx.doi.org/10.2139/ssrn.3547922.

[24] Pasquale Frank. The black box society: The secret algorithms that control money and information. Harvard University Press; 2015, http://dx.doi.org/10.4159/harvard.9780674736061.

[25] Gasser Urs. Recoding privacy law: Reflections on the future relationship among law, technology, and privacy. Harvard Law Rev Forum 2016;130:61, URL https://heinonline.org/HOL/Page?handle=hein.journals/forharoc130&id=62&div=&collection=.

[26] Hartzog Woodrow. Privacy's blueprint: the battle to control the design of new technologies. Harvard University Press; 2018, Google-Books-ID: YERMDwAAQBAJ.

[27] OECD. Regulatory effectiveness in the era of digitalisation. 2019, URL https://www.oecd.org/gov/regulatory-policy/Regulatory-effectiveness-in-the-era-of-digitalisation.pdf.

[28] Black Julia. The emergence of risk-based regulation and the new public management in the United Kingdom. Public Law 2005;2005(Autumn):512–49, URL http://www.sweetandmaxwell.co.uk/Catalogue/ProductDetails.aspx?recordid=469, Number: Autumn Publisher: Sweet & Maxwell Ltd.

[29] Breyer Stephen. Regulation and its reform. Harvard University Press; 1982, Google-Books-ID: HVgwEAAAQBAJ.

[30] Ogus Anthony I. Regulation: Legal form and economic theory. Bloomsbury Publishing; 2004, Google-Books-ID: onB6BAAAQBAJ.

[31] Mitnick Barry M. The political economy of regulation: creating, designing, and removing regulatory forms. Columbia University Press; 1980.

[32] Williamson David, Lynch-Wood Gary, Ramsay John. Drivers of environmental behaviour in manufacturing SMEs and the implications for CSR. J Bus Ethics 2006;67(3):317–30. http://dx.doi.org/10.1007/s10551-006-9187-1.

[33] Pelkmans Jacques, Renda Andrea. Does EU regulation hinder or stimulate innovation?. Rochester, NY; 2014, URL https://papers.ssrn.com/abstract=2528409.

[34] EUR-Lex. Precautionary principle - EUR-Lex. 2002, URL https://eur-lex.europa.eu/EN/legal-content/glossary/precautionary-principle.html.

[35] Thierer Adam D. Privacy law's precautionary principle problem. SSRN Electron J 2014. http://dx.doi.org/10.2139/ssrn.2449308.

[36] Solove Daniel. The three general approaches to privacy regulation. TeachPrivacy 2020. URL https://teachprivacy.com/the-three-general-approaches-to-privacy-regulation/.

[37] United Nations. Universal Declaration of Human Rights URL https://www.un.org/en/about-us/universal-declaration-of-human-rights, Publisher: United Nations.

[38] Hirvelä Päivi, Heikkilä Satu. 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. first ed.. Intersentia; 2022, http://dx.doi.org/10.1017/9781839703232.

[39] European Union Agency for Fundamental Rights. Article 7 - Respect for private and family life. Eur Union Agency Fundam Rights 2015. URL http://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life.

[40] European Union Agency for Fundamental Rights. Article 8 - Protection of personal data. Eur Union Agency Fundam Rights 2015. URL http://fra.europa.eu/en/eu-charter/article/8-protection-personal-data.

[41] United Kingdom. Data Protection Act 2018. 2018, URL https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted, Publisher: King's Printer of Acts of Parliament.

[42] CSRC Content Editor. NIST personal data - Glossary | CSRC. 2008, URL https://csrc.nist.gov/glossary/term/personal_data.

[43] Data Guidance. Comparing privacy laws: GDPR v. PIPL. 2021, URL https://www.dataguidance.com/sites/default/files/gdpr_v_pipl_.pdf.

[44] Buckley Gerard, Caulfield Tristan, Becker Ingolf. GDPR and the indefinable effectiveness of privacy regulators: can performance assessment be improved?. J Cyber Secur 2024. http://dx.doi.org/10.1093/cybsec/tyae017.

[45] Jin Ginger Zhe, Wagman Liad. Big data at the crossroads of antitrust and consumer protection. SSRN scholarly paper ID 3754671, Rochester, NY: Social Science Research Network; 2019, URL https://papers.ssrn.com/abstract=3754671.

[46] EC. The data protection directive 1995. Official J L 1995;281:0031–50, URL https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A31995L0046, Publisher: OPOCE.

[47] EU. Art. 1 GDPR – Subject-matter and objectives. 2018, URL https://gdpr-info.eu/art-1-gdpr/,

[48] EC. General data protection regulation one year on. Eur Commission - European Commission 2019. URL https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2956.

[49] Wikipedia. Big Tech. Wikipedia 2024. URL https://en.wikipedia.org/w/index.php?title=Big_Tech&oldid=1200526962, Page Version ID: 1200526962.

[50] Espinoza Javier. Fighting in Brussels bogs down plans to regulate Big Tech. 2021, URL https://www.ft.com/content/7e8391c1-329e-4944-98a4-b72c4e6428d0,

[51] EC. The Digital Markets Act: ensuring fair and open digital markets - European Commission. 2024, URL https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

[52] EC. The EU's Digital Services Act. 2024, URL https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

[53] EC. Data Act | Shaping Europe's digital future. 2023, URL https://digital-strategy.ec.europa.eu/en/policies/data-act.

[54] EC. Commission welcomes political agreement on artificial intelligence act | shaping Europe's digital future. 2023, URL https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-artificial-intelligence-act.

[55] EC. Proposal for an ePrivacy regulation | shaping Europe's digital future. 2024, URL https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation.

[56] Madison James. Fourth amendment | congress.gov | library of congress. 1792, URL https://constitution.congress.gov/browse/amendment-4/.

[57] Cornell Law school. Privacy, LII / Legal Information Institute, URL https://www.law.cornell.edu/wex/privacy.

[58] US Supreme Court. Estelle T. GRISWOLD others Appellants, v. state of connecticut. 1965, URL https://www.law.cornell.edu/supremecourt/text/381/479.

[59] Crain Matthew. The limits of transparency: Data brokers and commodification. New Media Soc 2018;20(1):88–104. http://dx.doi.org/10.1177/1461444816657096, Publisher: SAGE Publications.

[60] MIT Technology Review. What are the hardest problems in tech we should be more focused on as a society? MIT Technol Rev 2023. URL https://www.technologyreview.com/2023/11/01/1081939/big-questions-problem-solving-bill-gates-jennifer-doudna-lina-khan/.

[61] Emch Adrian. Antitrust and the Internet: Is China Different. Competit Law Int 2019;15(2):167–74, URL https://heinonline.org/HOL/P?h=hein.journals/cmpetion15&i=165.

[62] Hille Kathrin. 'Like it was with Jack Ma': China puts world's biggest Apple supplier in its crosshairs. Financial Times 2023. URL https://www.ft.com/content/47903211-8fbe-49ac-8f15-c3d9aa098397.

[63] Zhu Julie, Zhai Keith, Leng Cheng. How billionaire Jack Ma fell to earth and took Ant's mega IPO with him. Reuters; 2020, URL https://www.reuters.com/article/idUSKBN27L2GW/.

[64] Liu Lizhi. The Rise of Data Politics: Digital China and the World. Stud Compar Int Develop 2021;56(1):45–67. http://dx.doi.org/10.1007/s12116-021-09319-8.

[65] China Law Translate. Data security law of the PRC. China Law Transl 2021. URL https://www.chinalawtranslate.com/datasecuritylaw/.

[66] Orrick. China's new data security law: What international companies need to know. 2021, URL https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know.

[67] National People's Congress of the People's Republic of China (NPC). Personal Information Protection Law of the People's Republic of China. PIPL 2021. URL https://personalinformationprotectionlaw.com/.

[68] Peoples Republic of China. Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). DigiChina 2017. URL https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

[69] Doug [R-GA-9 Rep] Collins. H.R.4943 - 115th Congress (2017–2018): CLOUD act. 2018, URL https://www.congress.gov/bill/115th-congress/house-bill/4943, Archive Location: 2018-02-06.

[70] China Briefing. PIPL vs GDPR - Key Differences and Implications for Compliance in China. China Brief News 2022. URL https://www.china-briefing.com/news/pipl-vs-gdpr-key-differences-and-implications-for-compliance-in-china/.

[71] Skadden. China's new data security and personal information protection laws: What they mean for multinational companies | insights | skadden, arps, slate, meagher & flom LLP. 2021, URL https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws.

[72] EUR-Lex. 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. 2024, URL http://data.europa.eu/eli/reg/2024/1689/oj/eng, Legislative Body: CONSIL, EP.

[73] Aguilar Francis Joseph. Scanning the business environment. Macmillan; 1967, Google-Books-ID: sn1EAAAAIAAJ.

[74] Boult M. Horizon scanning: A practitioner's guide. Tech. rep., Institute of Risk Management; 2018, URL https://pure.roehampton.ac.uk/ws/portalfiles/portal/1155531/Horizon_scanning_final2.pdf.

[75] European Commission. Context analysis – PESTEL. 2018, URL https://wikis.ec.europa.eu/pages/viewpage.action?pageId=50109048.

[76] Battista Michelle. CIPD | PESTLE analysis. CIPD 2024. URL https://www.cipd.org/uk/knowledge/factsheets/pestle-analysis-factsheet/.

[77] Data governance challenges. In: Global governance futures. first ed.. London: Routledge; 2021, p. 238–52. http://dx.doi.org/10.4324/9781003139836-21, URL https://www.taylorfrancis.com/books/9781003139836/chapters/10.4324/9781003139836-21.

[78] Vogel David. Trading up: Consumer and environmental regulation in a global economy. Harvard University Press; 2009, Google-Books-ID: 6MOpRPxp5L0C.

[79] Bradford Anu. The brussels effect: How the european union rules the world. Oxford University Press; 2020, Google-Books-ID: vb7xxwEACAAJ.

[80] Bradford Anu. Digital empires: the global battle to regulate technology. Oxford University Press; 2023, Google-Books-ID: ibnQEAAAQBAJ.

[81] Fisk Joel. EU-US Data Privacy Framework: 3rd time lucky? Outsourced Data Protect Officers GDPR Data Prot Compliance 2023. URL https://www.dpocentre.com/eu-us-data-privacy-framework-3rd-time-lucky/.

[82] Snowden Edward. Snowden Archive. CJFE | Can J Free Expr 2015. URL https://www.cjfe.org/snowden.

[83] Interesse Giulia. A comprehensive analysis of the European GDPR and evolving Chinese data protection laws. Eur Guanxi 2023. URL https://www.europeanguanxi.com/post/a-comprehensive-analysis-of-the-european-gdpr-and-evolving-chinese-data-protection-laws.

[84] de Her Paul, Papakonstantinou Vagelis. The data protection regime in China. Eur Parliament 2015. URL https://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPO_IDA%282015%29536472_EN.pdf.

[85] Politico. Deal over dim sum: China caves to EU on data to keep investors sweet. Politico 2023. URL https://www.politico.eu/article/deal-over-dim-sum-china-caves-eu-data-keep-investors-sweet/.

[86] Voss W Gregory, Bouthinon-Dumas Hugues. EU general data protection regulation sanctions in theory and in practice. SSRN scholarly paper ID 3695473, Rochester, NY: Social Science Research Network; 2021, URL https://papers.ssrn.com/abstract=3695473.

[87] Fiveash Kelly. Viv Reding: That French Google fine? Pfft - it's pocket money, URL https://www.theregister.com/2014/01/21/viviane_reding_says_google_cnil_fine_is_pocket_money/.

[88] Wodinsky Shoshana. The Hidden Failure of the World's Biggest Privacy Law. Gizmodo 2022. URL https://gizmodo.com/gdpr-iab-europe-privacy-consent-ad-tech-online-advertis-1848469604.

[89] Nast Condé. How GDPR is failing. Wired UK 2022. URL https://www.wired.co.uk/article/gdpr-2022, Section: tags.

[90] Buckley Gerard, Caulfield Tristan, Becker Ingolf. 'It may be a pain in the backside but...' insights into the resilience of business after GDPR. In: Proceedings of the 2022 New Security Paradigms Workshop. 2022, p. 21–34. http://dx.doi.org/10.1145/3584318.3584320.

[91] nyob. Data protection day: 41 years of 'compliance on paper'?!. 2022, URL https://noyb.eu/en/data-protection-day-41-years-compliance-paper.

[92] Johnny Ryan Alan Toner. New data on GDPR enforcement agencies reveal why the GDPR is failing. Tech. rep, Brave; 2020, URL https://brave.com/dpa-report-2020/.

[93] The George Washington University Regulatory Studies Center. Regulatory compliance burdens literature review & synthesis. 2022, URL https://regulatorystudies.columbian.gwu.edu/sites/g/files/zaxdzs4751/files/2022-10/regulatory_compliance_burdens_litreview_synthesis_finalweb.pdf.

[94] Broadbent Meredith. The digital services act, the digital markets act, and the new competition tool. 2020, URL https://www.csis.org/analysis/digital-services-act-digital-markets-act-and-new-competition-tool.

[95] Rahnama Hossein, Pentland Alex Sandy. The new rules of data privacy. Harv Bus Rev 2022. URL https://hbr.org/2022/02/the-new-rules-of-data-privacy, Section: Data management.

[96] Georgetown University. Fleshing out St Augustine. 2024, URL https://faculty.georgetown.edu/jod/texts/sundayheraldreview.html.

[97] European ParliamentDirectorate General for Parliamentary Research Services. Blockchain and the general data protection regulation: Can distributed ledgers be squared with European data protection law?. LU: Publications Office; 2019, URL https://data.europa.eu/doi/10.2861/535.

[98] European ParliamentDirectorate General for Parliamentary Research Services. The impact of the general data protection regulation on artificial intelligence. LU: Publications Office; 2020, URL https://data.europa.eu/doi/10.2861/293.

[99] Narayanan Arvind, Shmatikov Vitaly. How to break anonymity of the Netflix prize dataset. 2007, URL arXiv:cs/0610105.

[100] Rocher Luc, Hendrickx Julien, Montjoye Yves-Alexandre. Estimating the success of re-identifications in incomplete datasets using generative models. Nature Commun 2019;10. http://dx.doi.org/10.1038/s41467-019-10933-3.

[101] Tene Omer, Polonetsky Jules. Big data for All: Privacy and user control in the age of analytics. Northwestern J Technol Intellectual Property 2012;11(5):[xxvii]–274, URL https://heinonline.org/HOL/P?h=hein.journals/nwteintp11&i=268.

[102] Hoepman Jaap-Henk. Privacy is hard and seven other myths: Achieving privacy through careful design. MIT Press; 2021, Google-Books-ID: 7GFBEAAAQBAJ.

[103] Wikipedia. Regulatory technology. Wikipedia 2024. URL https://en.wikipedia.org/w/index.php?title=Regulatory_technology&oldid=1167034194, Page Version ID: 1167034194.

[104] Eggers Dave. The circle. Knopf Doubleday Publishing Group; 2013, Google-Books-ID: sbxWAAAAQBAJ.

[105] Eggers Dave. The every. Knopf Doubleday Publishing Group; 2021, Google-Books-ID: hbAeEAAAQBAJ.

[106] Parikh Tej. Erik Brynjolfsson: 'This could be the best decade in history — or the worst'. Financial Times 2024. URL https://www.ft.com/content/b71759fe-397b-4688-bc81-b082edb25f31.

[107] Yale School of the Environment. As Use of A.I. soars, so does the energy and water it requires, Yale E360. 2024, URL https://e360.yale.edu/features/artificial-intelligence-climate-energy-emissions.

[108] Hodgson Camilla, Kinder Tabby. Microsoft's and Google's AI plans clouded by concerns of rising costs. Financial Times 2024. URL https://www.ft.com/content/a062df1d-aaf5-4604-8f97-4444170482f2.

[109] CJEU. The CJEU judgment in the Schrems II case. 2020, URL https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

[110] US Department of Justice. The Foreign Intelligence Surveillance Act of 1978 (FISA) | Bureau of Justice Assistance, URL https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286.

[111] Murgia Madhumita. Google moves UK user data to US to avert Brexit risks. Financial Times 2020. URL https://www.ft.com/content/135e5b66-53fb-11ea-90ad-25e377c0ee1f.

[112] Tuta Hanna. UK Gmail users to lose EU data protection. Tutanota URL https://tuta.com/blog/posts/uk-gmail-users-lose-eu-data-protection.

[113] Koski Heli, Valmari Nelli. Short-term impacts of the GDPR on firm performance. Working paper 77, ETLA Working Papers; 2020, URL https://www.econstor.eu/handle/10419/237362.

[114] Buckley Gerard, Caulfield Tristan, Becker Ingolf. GDPR: is it worth it? perceptions of workers who have experienced its implementation. 2024, http://dx.doi.org/10.48550/arXiv.2405.10225, URL arXiv:2405.10225[cs].

[115] Manancourt Vincent. EU privacy law's chief architect calls for its overhaul. Politico 2021. URL https://www.politico.eu/article/eu-privacy-laws-chief-architect-calls-for-its-overhaul/.

[116] Reding Viviane. Keynote speech by viviane reding | European data protection supervisor. 2024, URL https://www.edps.europa.eu/press-publications/press-news/videos/keynote-speech-viviane-reding.

[117] noyb. GDPR: a culture of non-compliance?. 2024, URL https://noyb.eu/sites/default/files/2024-01/GDPR_a%20culture%20of%20non-compliance_2.pdf.

[118] Hijmans Hielke. How to enforce the GDPR in a strategic, consistent and ethical manner discussion. Eur Data Protect Law Rev (EDPL) 2018;4(1):80–4, URL https://heinonline.org/HOL/P?h=hein.journals/edpl4&i=86.

[119] Liu Qianer. China to lay down AI rules with emphasis on content control. Financial Times 2023. URL https://www.ft.com/content/1938b7b6-baf9-46bb-9eb7-70e9d32f4af0.

[120] Wikipedia. Pegasus (spyware). Wikipedia 2024. URL https://en.wikipedia.org/w/index.php?title=Pegasus_(spyware)&oldid=1210945241, Page Version ID: 1210945241.

[121] Katie Prescott Editor Technology Business. Getting tough on AI could backfire on European Union. 2024, URL https://www.thetimes.co.uk/article/getting-tough-on-ai-could-backfire-on-european-union-p2dxr50zd.

[122] Volpicelli Gian. France means business with Mistral-Microsoft deal. Politico 2024. URL https://www.politico.eu/article/why-france-chose-to-be-europes-ai-playground/.