Comparative Analysis of Global Data Protection Models: Market-Driven, State-Driven, and Rights-Driven Approaches

Shuq Hussein[1*]

[1] *University of Edinburgh, Edinburgh Law School, United Kingdom*
E-mail:shuqhussen91@hotmail.com
(Received: Feb 16, 2025, Revised: Mar 18, 2025, Accepted: Mar 26, 2025, Published: Mar 30, 2025)

Abstract: Around the world, three digital emphases for protecting personal data exist: the US market-driven regulator model, the Chinese state-driven model, and the EU rights-driven regulator model. These three approaches shape society, individuals' lives, and our digital economy. In liberal democracies with mature market systems, digital technology has generated immense economic value and empowered individuals in the public sphere. This paper examines these regulatory models through the lens of three key principles: the right to be forgotten, privacy by design, and data minimization.

Keywords: GDPR, data protection, EU, USA, China.

I Background for Three Digital Regulatory Models

In the USA, regulatory frameworks applied to digital platforms and enterprises have been addressed through specific, additional regulations for different sectors of activity. This creates a patchwork of sector-specific regulation instead of general, specifically digital regulation. Many regulations were developed before the internet emerged as an essential factor or do not contemplate technological developments. In the United States (US), there are regulations at state and federal levels that address the legal issues around privacy and protect personal data in different fields, such as Healthcare, financial information, and others for vulnerable groups like children. This is unlike the EU and China, which have comprehensive regulations that address all the legal issues of personal data production (1). On the state level, California became the first state to have comprehensive law for data protection issues in 2018, effective in 2023, then Virginia, Colorado, and Utah. The federal state began with the Privacy Act of 1974, which regulates the federal agencies handling the personal data of individuals; then, in the eighth years, when technology started to advance(2), President Clinton issued different privacy regulations such as the Health Data Protection Bill (The Health Insurance Portability and Accountability Act (HIPAA) of 1996) which protects patient data in medical institutions and prevents the used his data without expediency consent(3), 2- the financial data protection to protect the consumer from and financial data breach of threat and to regulate the used his sensitive data from the bank and other financial institution by (Gramm-Leach-Bliley Act (GLBA) of 1999)(4) where the data protection law for the children the Children's Online Privacy Protection Act (COPPA) of 1998 and regulate used this data and transfers. So, this is the patchwork of different laws shaping the legal framework of the US approach to data protection (5). While new technologies bring new issues and challenges, such as privacy, net neutrality, cyber terrorism, and monopolies, the USA has long held that specific business models or types of disruptions are not more important than established legal principles and values, such as free speech, security, integrity, availability, and privacy of private communications. Market-Driven Regulation(6). Market-driven approaches aim to facilitate the creation of privately imposed rules, allowing market actors to self-regulate. Market-driven approaches to digital enterprise regulation are concerned with laws and regulations that achieve their aims by encouraging better overall adherence to those rules through market mechanisms(7). A fundamental aspect of most market-driven regulatory approaches is that they allow for more flexible and adaptable rule making than traditional government regulation. Although the government can manage or shape market-driven regulation outcomes, the core of market-driven regulation is that private actors remain responsible for developing the specific norms

and rules of self-regulation.(8) The state in China plays a central part in the administration of digital market activities. In China, it is not the market's integration that defines digital regulatory strategies; it is state-driven unfolding. It takes a centralized regulatory model, marked by top-down policy formulation that prioritizes state interests above all. Regulatory measures, whether surveillance-related administrative orders or softer normative ones, are crafted to align with and advance national goals, such as economic development and social stability. Security and stability concerns also motivate a proactive regulatory stratagem that extends to the early-stage control of technological development to prevent potential risks and problems subsequently.(9) It has mentioned how the permeation of the internet maps into daily lives presents challenges for China's surveillance. Firms with digital interest are singled out and sternly reminded to be wary of the regulatory risks when engaging in location-based services. On the other hand, firms' terms of the MOC's imposed conditions must refrain from setting up a plan or network that impairs the national interest in border, sovereignty, and location security.(10) Domestic firms adapt to the regulatory model; the Chinese digital firms retained remarkable compliance compared to other foreign companies entering the market (11). Compliance with the anti-money law also demonstrates substantial conformity with the Chinese digital model to avoid penalties being fixed on other foreign players. Original domestic concerns motivated the compatibility of the business model to remain operational in a controlled environment. Ending investigation after minor restructuring. Yet, regarding consumer privacy, the framing of privacy regulations has not solidified domestic firms' ability to acquire information within the legal context of data usage. The European Union is one of the leading players in global trade and, simultaneously, the region with the highest levels of privacy and data protection as fundamental rights(12). The principal legal act in the EU data protection field is the General Data Protection Regulation, whose scope applies to all companies that process the personal data of European citizens (13). The GDPR is a regulation that has been in force since May 2018 that protects personal data within the EU and the European Economic Area, and it also governs the transfer of data outside of those areas. The regulation was designed to harmonize and update data protection rules and contain rights for individuals whose personal data is being processed. It was designed to empower individuals and outline the context and conditions for processing personal data.(14) To this end, some specific rules were applied to businesses that provide information services and operate in the field of electronic commerce, given the specificity of their activities, i.e., the manner, reasons for, and conditions under which personal data is processed for the main activity of an information society service provider (15). The GDPR sets forth the measures that companies operating in electronic commerce must undertake to ensure the transparency, purpose limitation, data minimization, storage limitation, and accuracy of the data they process(16). These measures aim to impose on companies processing personal data the obligation to provide proof of compliance with their privacy obligations to the National Data Protection Authorities and to demonstrate their compliance (17). This essay will examine the position of each regulatory model on different EU privacy principles, such as data minimization (Art.5 (1/c), the right to be forgotten (Art. 17), and privacy by design (Art. 25). We will examine how these privacy principles support the fundamental rights of individuals and how they conflict with the US and Chain approach.

II Right to be forgotten principle

Article 17 of GDPR ensures that individuals can request to erase and forget their data from the internet. The right to erase is a request from the data subject to the controller to remove his data, and the right to forget is an obligation on the controller to ask other controllers or processors—who share the data with him—to remove the data of the data subject from their website (18). The comment case for (the right of forgotten) is case No: 131/12 between Google Spain v AEPD and Mario Costeja González in 2014, which was considered the first transforming point to adopt the (right of forgotten) in article 17 in the GDPR, as this right was absent on the first draft of the GDPR. As Mario is a Hispanic citizen, he complained that his research name on Google found some old links and information about real state auctions on his property for old financial issues. This information was no longer relevant

and caused reputation harm for him; based on that, he asked the Spanish Data Protection Agency (AEPD) to remove these links from the Google edging. Based on that, the EU Court of Justice rulings that (search again as Google must remove unnecessary data for individuals, based on the balance between the right of privacy for the data subject and the right to access the information from the citizen, and the search engine should comply with the data protection directive 1995 event is located outside of the EU if they provided service in EU territory (19). The original version of the right of forgotten, which the EU Commission suggested, is different from the last version of Article 17 (2) as the original version. It would have had more strength for the controller, which obligated the controller to be responsible for the data of the data subject being removed from the website if he shared the data with third parties. At the same time, the last GDPR version asked the controller to take reasonable steps to ensure the data subject's data was removed from the website(18). Unless this data exemption is removed because it is considered of public interest, such as public health, it is necessary for historical or scientific research or statistical purposes according to article 89 (1) of GDPR. The Chinese Personal Information Protection Law (PIPL) 2021 is closed to the legal principles under GDPR. It addresses the right to be forgotten under Article 47, which gives the data subject the right to request that his data be deleted in specific circumstances, such as when the purpose of processing has been fulfilled or if the data subject withdrew his consent(20). Additionally, the article mandates that if the technical measure prevents data from being deleted, the controller should stop processing the data, and he can store the data as an alternative measure. This leads us to say that the (right to be forgotten) under GDPR is more proactive in supporting the fundamental right by cantering on data subject autonomy and expediency consent. At the same time, article 47 of chain PIPL is about post-processing remedies with less emphasis on empowering individuals through consent-based control(20). The right to be forgotten is not comprehensively regulated under US privacy laws; as data protection law in California, some privacy laws regulate the right to delete data, especially for voluntary groups, like children's or consumer data. Under California Consumer Privacy Act 2018, Article (1798.105), the consumer has the right to request that the businesses delete his information unless the business legally requests to keep this information, to complete the transaction for which the data was collected, or any other perform contract between the consumer and business(2).

III Privacy by design principle

Using tech regulation to protect individuals' freedom and fundamental rights is a core feature of the EU rights-driven regulator model. Article 2 of the EU treaty states, "The Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities(21)." The GDPR, recital 1, considers the protection of personal data through processing data and concedes it as a fundamental right(22). The term privacy by design was used for the first time in 1995 in the report Privacy-enhancing Technologies: The Path to Anonymity)(23); Also, Directive 95/46/EC data protection directive talks about the principles of privacy by design under article 17/1, titled Security of processing, and this article requires implementing appropriate technical and organizational measures to protect personal data(24). However, before the privacy by design principle, the organization addressed the privacy breach after harming the data subjects; this increased the privacy issues until this principle was adopted under Article 25 of GDPR(25). Privacy by design principle conceded one of the core principles under the GDPR, supports the fundamental right for individuals to be forgotten) and (data minimization) principles(14). This was clearly from the seven fundamental principles for the PbD (see Figure 1)(26):

1. Proactive approach: This means preventing data breaches before they happen, as this high-level and clear commitment to protecting the user's data before using the technology.
2. Privacy by default: There is no need to adopt any privacy measure to protect individual data; the system protects it by default. This system ensures that only the necessary data is collected for limited purposes after the individuals' expediency consent, and the unnecessary data is safely

destroyed(27).

3. Privacy embedded in design: This principle supports including privacy measures in IT systems in a holistic, creative, and integrative way. This inclusive approach strengthens the protection of rights across different groups, including vulnerable or minority populations, in line with values of equality and dignity(27).
4. Full function, Positive sum, not zero-sum: All goals and interests should be explicitly recorded, preferred functionalities defined, and matrices established and utilized. Compromises are typically rejected as superfluous in favor of seeking a solution that supports multi-functionality(27).
5. Life-cycle protection: The privacy measure was embedded from the beginning in the AI system, protecting the individuals' data from day one on the system and continuing throughout the system's life cycle or until the data is destroyed. This principle supports the idea that there is no privacy without strong security.(14)
6. Transparency and visibility: Privacy by design entails the duty to care for individuals' data, establish redress and complaints mechanisms, and explain how to access these mechanisms and processes to protect their data. This is considered a strong guarantee of protecting individuals' fundamental rights
7. Respect user privacy: This emphasizes and prioritizes privacy by prioritizing the individual's interests through substantial privacy defaults, clear notices, and empowering, user-friendly options.(28)

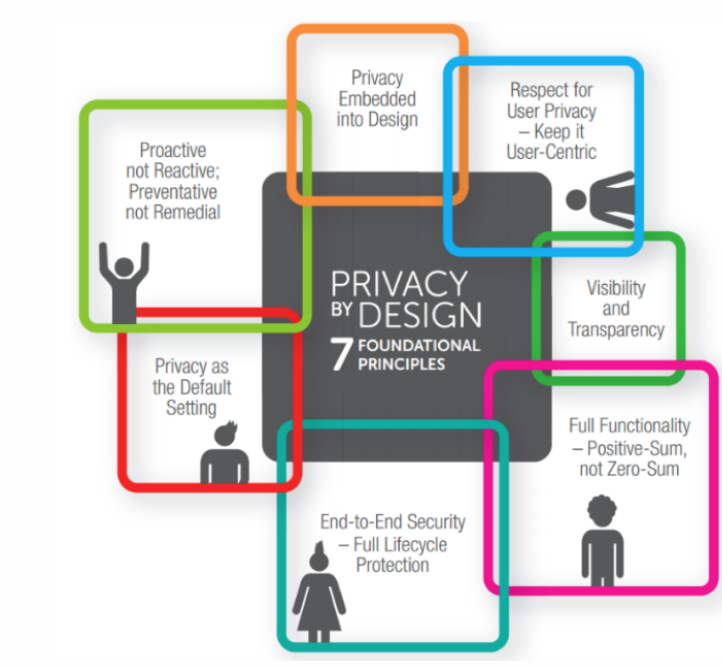

Figure 1: The seven foundation principles for privacy by design(29)

As it was clear that privacy is by design, how is the priority for protecting the individual's data more than the business development or civilians for the state? In the US, there was no comprehensive bill addressing privacy issues at the federal level; the US Supreme Court of Justice ruled that privacy was (to keep the person alone) in 1890; after 100 years, Privacy by Design (PbD) was introduced in the 1990s by Dr. Ann Cavoukian, then Ontario's Information and Privacy Commissioner, as a proactive response

to emerging online privacy threats. In 2010, momentum grew in the European Union, where the Article 29 Data Protection Working Party advocated incorporating PbD principles into EU regulations, later echoed by the European Data Protection Supervisor. In the US, the Federal Trade Commission (FTC) hosted privacy round-tables in 2009 and 2010, culminating in a 2012 report that recommended privacy by design as a core business framework. By 2011, PbD appeared in federal legislation through Senators John Kerry and John McCain's proposed Commercial Privacy Bill of Rights, signifying its growing importance in shaping privacy regulations worldwide(30). This bill is considered the first to address the privacy by design principle in the US. This principle obligates businesses to develop tech products to help consumers understand how they work, collect, process, and store their data(10). But when we go to the practical, we see that the president of Sun Micro-systems said in 1999: (You have zero privacy anyway, get over it) this expediency expressed that the large company was not interested in protecting the ordinary data for the individuals, though the company used some technology to protect the privacy of the individuals by using technology that prevents acquiring not only data from the consumer, like:but the government it is still the problem to regulate and monitor the privacy of individuals and apply satanic for breach and violation. Apple, for example, proactively incorporates an approach to protect children from illegal activities without legal obligation from the US government. This approach contrasts with the EU approach, which obligates the tech company to integrate the technology to achieve and protect the individual's privacy by design based on a regulatory framework to enforce the same outcomes. No article in PIPL chain 2021 addresses the privacy by design principle as article 25 in GDPR. Still, Chapter V in PIPL enacted some reactive mechanisms and some obligations for the processor to ensure the protection and the security of the individual's information according to Article 59, As Article 51 outlines measures to ensure the processing of the information compliance with the law and prevent the unauthorized visit, or leakage or loss the personal data. If that happens, article 57 encourages the data controller to take remedial measures to protect personal data. However, the PIPL Still operates within a context where individual rights may be secondary to government surveillance and data sovereignty concerns.

Comparative analysis shows:

Region	**Implementation**
EU	Strong right with public interest exceptions
China (PIPL Art.47)	Limited right, secondary to state interests
US (CCPA)	Sectoral right with broad exemptions

Table 1: Right to be forgotten across jurisdictions

IV Data Minimization Principle

The data minimization principle came from Article 6 (1/c) Directive 95/46/EC of the data protection directive in 1995, Article 6: 1. Member States shall provide that personal data must be: a) adequate, (b) relevant and (c) not excessive about the purposes for which they are collected and/or further processed; After that, the GDPR replaced the excessive phrase (limited to what is necessary) in Article 5 (1)(31) (c) of GDPR(1). Article 5/c "adequate, relevant and limited to what is required about the purposes for which they are processed. The U.S. adopts a market-driven approach to privacy regulation, where data minimization is more of a recommendation than a stringent requirement. Phrases like "If you don't need it, don't store it" are legal principles that guide developers and businesses in collecting only necessary data. The California Consumer Privacy Act (CCPA), particularly Section 1798.100(a)(1)(2), attempts to align with this principle by preventing businesses from collecting additional information or using data for purposes other than those disclosed initially without consumer consent(32). However, the dominance of tech companies like Meta and Google, which rely on massive data collection to support their advertising-driven business models, undermines the efficacy of such regulations. Although the CCPA offers a framework, companies frequently prioritize profit over privacy, and enforcement

and adherence are still uneven. Due to loopholes that allow firms to obtain wide user consent for data gathering and use that data for different purposes, the U.S. approach fails to strictly enforce data minimization. This strategy puts market efficiency and innovation ahead of individual privacy, which leads to a large amount of data being collected that goes against the fundamental idea of data minimization(15). In the chain, Article 6 of PIPL law 2021 states that (..... Personal information shall be collected only to the minimum scope for processing, and excessive collection of personal information shall not be allowed). This substantially resembles the GDPR(20). But this legal provision is in sharp contrast to reality. Without getting people's permission, the Chinese government frequently gathers personal information through surveillance and facial recognition technologies. This data violates the minimization principle because it is kept permanently and can be exploited for political objectives(20).

China's strategy integrates data collecting into the very fabric of governance, prioritizing social stability and state control more than individual liberties. In addition to undermining fundamental rights, the widespread use of personal data for monitoring exposes a serious disconnect between legal theory and practice. The EU, in contrast, centers individual rights at the center of its regulatory framework. The GDPR ensures strict adherence to the data minimization principle, fostering trust and accountability. By requiring organizations to justify data collection and limit it to specific purposes, the EU creates a balanced environment that protects privacy without stifling innovation.

V Balance the interest

It's complex for the regulator to balance the interests of individuals, businesses, and states in the context of legal principles of data protection. As we have seen, Neither a purely market-driven model in the US, the right-driven model in the EU, nor a state model in the chain is entirely sufficient on its own. In my opinion -with difficulty in applying- the hybrid approach that integrates the strength of each system is likely the most effective way to balance these competing interests, and would prioritize privacy and innovation the business interest, and all the stakeholders benefit from the digital economy. The EU's regulatory framework, particularly the GDPR, provides a strong foundation for protecting individual rights and ensuring ethical data practices. Its emphasis on data minimization, purpose limitation, and user consent gives individuals greater control over their personal data. Additionally, the EU's focus on responsible AI development ensures that technological advancements align with societal values and human rights. However, the EU's approach can sometimes be criticized for being overly rigid, potentially stifling innovation and creating compliance burdens for smaller businesses. On the other hand, the US model has more flexibility, but the lack of stringent federal regulations allows firms to experiment and adapt quickly, rapid the tech advancements. However, this approach often fails to protect individuals' data as the EU, and this leads to mistrust and potential harm to the data subject. In chain, the regulation represents the state-driven model, that the state plays the commanding role in developing the privacy of the individuals. This model takes national security, social stability, and economic development has enforced broad data localization and surveillance policies across the country to monitor and manage information coming in and going out of their boards, while this model does ensure rapid tech development and top-down decision-making processes, it seriously raises a series of human rights and freedom of expression concerns and serious question about the data breach and misuse of AI system. The state-driven model also seriously encroaches upon businesses' and individuals' agency, making innovation dependent upon government priorities and not necessarily dependent on market dynamics or other societal needs. A hybrid approach would combine the strengths of these models while mitigating their weaknesses. It would establish robust but flexible regulations that set a baseline of privacy protections, such as data minimization and transparency, while allowing businesses the freedom to innovate within these boundaries. A risk-based compliance framework could ensure that stricter measures are applied to high-risk data processing activities, such as the use of sensitive personal data or AI systems with significant societal impact, while providing more leeway for low-risk activities. This approach would also incentivize ethical practices by encouraging businesses to adopt privacy-by-design principles and embedding data protection into the development of products

and services from the outset. Public-private partnerships could further foster collaboration between governments, businesses, and civil society to develop ethical guidelines and share best practices.

Empowering individuals is another critical component of a balanced approach. Investing in digital literacy and public awareness campaigns would equip individuals with the knowledge to protect their privacy and exercise their rights. Tools like data portability, access rights, and the ability to opt out of data collection would give individuals greater control over their personal information. Additionally, accessible and efficient redress mechanisms would ensure that individuals can seek justice in cases of privacy violations. Balancing innovation with societal interests is equally important. Ethical AI frameworks that prioritize fairness, accountability, and transparency would ensure that AI systems benefit society as a whole. Encouraging businesses to share anonymized data for research and public interest purposes, such as healthcare or climate change, would further align commercial interests with societal needs. States play a crucial role in this hybrid approach by setting and enforcing privacy standards while supporting innovation through funding, research, and infrastructure development. International cooperation is also essential to address cross-border challenges and prevent regulatory fragmentation. States must strike a balance between national security interests and individual privacy rights, ensuring that surveillance and data collection practices are proportionate and subject to oversight. By fostering collaboration, empowering individuals, and promoting ethical practices, this hybrid approach can create a digital ecosystem that respects privacy, drives innovation, and benefits society as a whole.

In conclusion, a hybrid approach that combines the EU's emphasis on privacy and human rights, the US's focus on innovation and market dynamics, and the state-driven regulatory elements seen in China—while mitigating their respective weaknesses—is the most suitable way to balance the interests of individuals, businesses, and states. This approach can ensure that all stakeholders thrive in the digital age while safeguarding fundamental rights and promoting ethical practices by finding the right balance between regulation, market freedom, and state oversight. The key lies in fostering collaboration, empowering individuals, and creating a framework that prioritizes both innovation and societal well-being. Privacy is a fundamental right closely related to human dignity and the core values of integrity and confidentiality. Privacy considerations necessarily intersect with commercial interests and business operations. Companies are increasingly collecting data about the usage of their products, services, and interactions, and this data collection does not always align with privacy protection considerations. One study that argues that 50 percent of Americans did not trust the federal government and social media sites to protect their data- see Figure 2- high-profile data breaches, misuse of personal information, and the lack of transparency in data handling practices have eroded public trust. When users feel their data is not secure, they are less likely to engage with digital services, which can ultimately harm businesses.

Data collection practices can be motivated by different intentions, varying from good business performance and the legitimate quest for profit to less persuasive motivations such as watching undesirable customer behavior(34). Data collection practices can also provide more useful customer insights, just as inaccurate and incomplete information about these practices spreads in a market and may make goods and services more expensive for all. Inversely, interested business actors point out that privacy concerns can be a pretext for protectionism, an obstacle to better services(3). Countless reasons for exogenous data minimization have nothing to do with respect for values and information about individuals, and they can still bank on this rhetoric(35). The EU conceded the importance of protecting people's fundamental rights to achieving responsible AI. This approach is right from the roots and will serve the humanities for a long time and achieve AI sustainability to allow humans to benefit from AI. It is more than the US and chain approach, which gives the market a different level—to control the humanities, and this will entirely be scared to maintain the machines on the human one day.

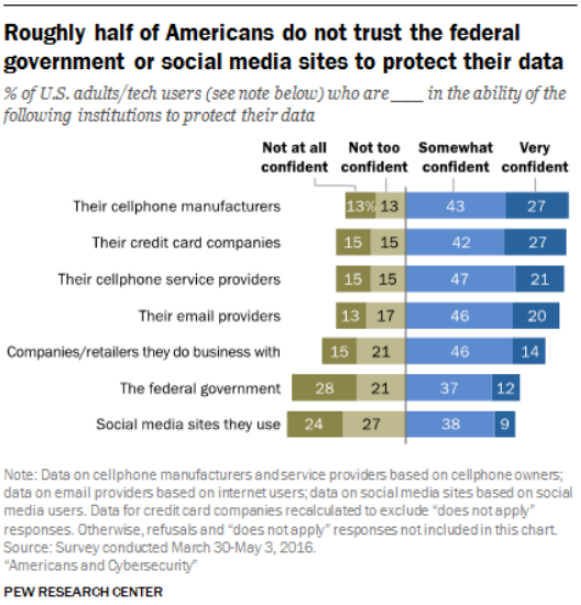

Figure 2: USA data protection(33)

VI Conclusion

In conclusion, The three principles presented -data minimization, privacy by design, and right to be forgotten- reverse the hierarchical list regarding who is best at creating the regulatory environment needed to support all actors and society the way the law intends, where the EU is far ahead of a market-driven U.S. alternative or a state-controlled Chinese alternative. When the EU incorporates privacy into its fundamental principles, it recognizes that individual rights matter and that privacy is not a mere policy choice but a fundamental human right. This method helps build trust and ensures accountability, where data is responsibly collected and used effectively while reducing unnecessary or intrusive practices.

References

[1] Tanusree Sharma, Lin Kyi, Yang Wang, and Asia J. Biega. "i'm not convinced that they don't collect more than is necessary": User-controlled data minimization design in search engines. In *Proceedings of the SEC '24: Proceedings of the 33rd USENIX Conference on Security Symposium , year = 2024.*

[2] California Legislative Counsel. Assembly bill no. 375: Chapter 55, civil code section 1798.100-1798.199, 2018.

[3] Lamya Alkhariji et al. Semantics-based privacy by design for internet of things applications. *Future Generation Computer Systems*, 138, 2023.

[4] Mathieu Gorge. Making sense of log management for security purposes - an approach to best practice log collection, analysis and management. *Computer Fraud and Security*, 2007(5), 2007.

[5] Miguel Villegas. *Privacy by Design for Web Developers.* 2024.

[6] Arunmozhi Manimuthu, V.G. Venkatesh, Yangyan Shi, V. Raja Sreedharan, and S.C. Lenny Koh.

Design and development of automobile assembly model using federated artificial intelligence with smart contract. *International Journal of Production Research*, 60(1), 2022.

[7] Kasia Zalewska-Kurek, Selim Kandemir, Basil G. Englis, and Paula Danskin Englis. Development of market-driven business models in the it industry. how firms experiment with their business models? *Journal of Business Models*, 4(3):48–67, 2016.

[8] David W. Cravens, Nigel F. Piercy, and Ashley Prentice. Developing market-driven product strategies. *Journal of Product & Brand Management*, 9(6):369–388, 2000.

[9] Kareem Othman. Public acceptance and perception of autonomous vehicles: A comprehensive review. *AI and Ethics*, 1(3), 2021.

[10] European Court of Auditors. The eu's response to china's state-driven investment strategy. Technical report, 2020.

[11] Rongxing Lu, Kevin Heung, Arash Habibi Lashkari, and Ali A. Ghorbani. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot. *IEEE Access*, 5, 2017.

[12] S.I. Tay, T.C. Lee, N.Z.A. Hamid, and A.N.A. Ahmad. An overview of industry 4.0: Definition, components, and government initiatives. *Journal of Advanced Research in Dynamical and Control Systems*, 10(14), 2018.

[13] Gerard Wilkinson. General data protection regulation: No silver bullet for small and medium-sized enterprises. *Journal of Payments Strategy and Systems*, 12(2):139–149, 2018.

[14] Ann Cavoukian. Privacy by design - the 7 foundational principles. Technical report, Information and Privacy Commissioner of Ontario, Canada, 2011.

[15] ICO. Data minimisation. Technical report, 2023.

[16] Matjaž Drev and Boštjan Delak. Conceptual model of privacy by design. *Journal of Computer Information Systems*, 62(5), 2022.

[17] Ben Wolford. Millions of small businesses aren't gdpr compliant, our survey finds. *GDPR.Eu*, 2019.

[18] European Data Protection Board. Guidelines 5/2019 on the criteria of the right to be forgotten in the search engines cases under the gdpr (part 1). Technical report, 2019.

[19] European Court of Justice. Google spain v. agencia española de protección de datos (aepd) and costeja gonzález, 2014. Case C-131/12.

[20] Yuxi Jin and Bernd Skiera. How do privacy laws impact the value for advertisers, publishers and users in the online advertising market? a comparison of the eu, us and china. *Journal of Creating Value*, 8(2), 2022.

[21] Cecilia Panigutti et al. The role of explainable ai in the context of the ai act. In *ACM International Conference Proceeding Series*, 2023.

[22] Philipp Hacker, Johann Cordes, and Janina Rochon. Regulating gatekeeper ai and data: Transparency, access, and fairness under the dma, the gdpr, and beyond. *SSRN Electronic Journal*, 2023.

[23] Peter Hustinx. Privacy by design: Delivering the promises. *Identity in the Information Society*, 3(2):253–255, 2010.

[24] Dag Wiese Schartum. Making privacy by design operative. *International Journal of Law and Information Technology*, 24(2), 2016.

[25] Daniele Ruggiu et al. Responsible innovation at work: Gamification, public engagement, and privacy by design. *Journal of Responsible Innovation*, 9(3), 2022.

[26] Ann Cavoukian. Privacy by design - the 7 foundational principles - implementation and mapping of fair information practices. Technical report, Information and Privacy Commissioner of Ontario, Canada, 2009.

[27] Ann Cavoukian. Operationalizing privacy by design: A guide to implementing strong privacy practices. Technical report, Information and Privacy Commissioner, Ontario, Canada, 2012.

[28] Ann Cavoukian. Privacy by design in law, policy and practice. a white paper for regulators, decision-makers and policy-makers. Technical report, Information and Privacy Commissioner, Ontario, Canada, 2011.

[29] Privacy by design: 7 fundamental principle. 2017.

[30] Ann Cavoukian. Understanding how to implement privacy by design, one step at a time. *IEEE Consumer Electronics Magazine*, 9(2), 2020.

[31] Lee A. Bygrave. Data protection by design and by default: Deciphering the eu's legislative requirements. *Oslo Law Review*, 4(2), 2017.

[32] Awanthika Senarath and Nalin Asanka Gamagedara Arachchilage. Understanding software developers' approach towards implementing data minimization. In *Woodstock '18: ACM Symposium on Neural Gaze Detection*, 2018.

[33] Americans and cybersecurity. 2016.

[34] Markus Wieshofer. Data privacy is not meta: Why facebook's foray into the metaverse could be flawed from the start. *Cardozo International & Comparative Law Review*, 2022.

[35] Giorgia Bincoletto. Data protection by design: From privacy by design to article 25 of the gdpr. In *Data Protection by Design in the E-Health Care Sector*, pages 37–166. Nomos Verlagsgesellschaft mbH & Co. KG, 2021.