Advances in Consumer Research
https://acr-journal.com/
Volume-3 | Issue-5 |May: 2026
Original Researcher Article

AI-Driven Consumer Profiling and Privacy Rights:Challenges under Emerging Data Protection Laws.

Dr M P Chandrika [1], Mehak Chadha[2], Kirti Jaggi[3], Priyanka Mangaraj[4], Mr. Rishabh Verma[5]
[1]Professor and Principal, S. C. Nandimath Law College, Bagalkot, Karnataka, India.
Email ID : Chandrikakurandwad72@gmail.Com
[2]Assistant Professor,University Institute of Legal Studies,Chandigarh University.
Email ID : Mehakchadha19@yahoo.Com
[3]Assistant Professor, Asian Law College.
Email ID : Kirtijaggi@gmail.Com
[4]Assistant Professor, Presidency School Of Law, Presidency University, Bengaluru.
Email ID : Priyankamangaraj96@gmail.Com
[5]Assistant Professor,TMCLLS, Teerthanker Mahaveer University, Moradabad

ABSTRACT
The fast evolution and penetration of Artificial Intelligence (AI) in commercial ecosystems has revolutionized how businesses capture, process and leverage consumer data. AI based consumer profiling, which includes behaviour tracking, forecasting and automated determination has enormous economic potential, but is also destroying basic privacy. This paper examines how the profiling capabilities of AI clash with the principles and values of data protection as articulated under contemporary data protection frameworks such as the "European Union's General Data Protection Regulation" (GDPR), the "California Consumer Privacy Act" as amended by the "California Privacy Rights Act" (CCPA/CPRA) and the "Digital Personal Data Protection Act, 2023" (DPDPA) in India.
The present research through doctrinal analysis, comparative legal methodology and empirical case studies, identifies six main challenge domains: (i) algorithmic opacity and the right to explanation; (ii) the legal adequacy of the consent frameworks; (iii) the cross-border data flows and the fragmentation of jurisdictions; (iv) profiling of sensitive and inferred attributes; (v); children's data in AI-powered environments and (vi) the emerging tension between AI innovation imperatives and privacy-by-design obligations. The paper proposes a policy toolbox which features harmonized international standards, algorithmic impact assessments and enforcement, and the identification of inferred data as a specific type of sensitive data. The main topic is the idea that current legal frameworks, which serve as the bedrock, are structurally deficient to cope with the "scale, velocity, and opacity of today's AI profiling systems"....
Keywords: Artificial Intelligence, Consumer Profiling, Data Protection, GDPR, CCPA/CPRA, DPDPA, Algorithmic Decision-Making, Privacy Rights, Big Data, Automated Profiling, Surveillance Capitalism.

INTRODUCTION:

The economy of the 21st century is a digital economy in which consumers are offered services tailored to their preferences and habits mainly in exchange for revealing their intimate preferences, habits, social relationships, health, financial and other behaviors. Within infrastructure, this exchange happens by way of Artificial Intelligence systems that push data to meaningful consumer profiles with far more granularity and speed than ever achieved before. Whether it's tailored ads or dynamic prices, or credit scores or political micro-targeting, AI-driven profiling is a key feature of both commercial and government decision making.

This technological revolution is outstripping protecting individualistic norm that was created. AI systems running in real time, at scale, and with limited transparency are increasingly threatening the right to privacy, which is recognized as an important human right in Article 12 of the "Universal Declaration of Human Rights", and included in many constitutional orders. The profiling exercise is no longer limited to declared data, but also inferred attributes and derived insights and even to probabilistic attributes that can be built from seemingly innocuous data points.

Some efforts have been made to address these challenges in data protection legislation. The most complete regulation in the area of automatic processing and profiling is the "European Union's General Data Protection Regulation" (GDPR), which entered into force on 25 May 2018. "The California Consumer Privacy Act" (CCPA) provides state-level rights to consumers regarding their personal information, and was enhanced in 2023 with the "California Privacy Rights Act" (CPRA). "The Digital Personal Data Protection Act 2023" (DPDPA) is a turning point for data governance in India, the biggest democracy. But there are significant gaps that remain.

2. AI-Driven Consumer Profiling: Mechanisms and Scope

Consumer Profiling via AI is not one-size-fits-all. It covers a variety of computational methods, from simple but often interpretable statistical models to unintuitive deep-learning models. The analysis of the technical substrate is integral to any worthwhile legal analysis.

2.1 Definitional Framework

The GDPR includes the concept of "profiling" within its definition of "automated processing" of personal data in Article 4(4) as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person". While the essential elements of this definition are valuable, they fall short of encapsulating the multiplicity of modern AI systems automation, the use of personal data, and assessment of personal aspects.

Modern AI profiling systems extend this definition at critical points in three aspects. First, they use information that could be non-personal when initially gathered, but is rendered personal through aggregating and inferring. Second, they create credentials known as "derived attributes" information about health, sexuality, political views and creditworthiness, among others, that the data subject didn't reveal. Third, they generate probabilistic rather than deterministic profiles, thus defying the binary (accurate or inaccurate) categorization.

2.2 Core Technical Mechanisms

2.2.1 Behavioral Analytics

Digital traces clicks dwell time, scroll patterns, purchase history and location data are collected over time and used to create longitudinal behavioral traces. That information is fed to machine learning classifiers, which categorize consumers into consumer disposable groups, to forecast consumer behaviour, and match the content to that. The size of data – its breadth and depth means that it can be profiled with degree of accuracy that is much greater than the machine can itself predict to the data subject.

2.2.2 Predictive Modelling

The predictive models are models that go beyond observed behaviour and allow them to infer some latent attributes, such as gradient boosting model, neural network, assembling etc. Examples include canonical predictions of political opinions from music listening habits or health status from grocery shopping. The inferences can be quite precise, and valuable for commercial purposes just for this reason: they show consumers much that they haven't explicitly said.

2.2.3 Natural Language Processing and Sentiment Analysis

Social media postings, transcripts from customer service calls, and product reviews are all examples of textual data that can be mined with large language models and sentiment analysis tools to gain insights into emotional states, life events and psychological dispositions. When these systems are merged with biometric and physiological data flows, profiles of incredible intimacy are generated, with serious possibilities of tampering and discrimination.

2.2.4 Graph Analytics and Social Network Analysis

With graph-based AI systems, relationships between social connections are mapped and attributes of nodes are inferred by their relationship to the graph. When the social network of a consumer shows characteristics that are linked with a specific demographic, medical condition or monetary behaviour, then those can be transferred to the individual, irrespective of their data. This mechanism goes against the grain of most data protection law, which has an individualistic perspective to it.

2.3 The Data Ecosystem Enabling Profiling

AI profiling is not done in a vacuum. It's all part of a larger framework of data that includes data collected by the marketer from consumers (first-party), data shared by other marketers with whom the marketer has a commercial relationship (second-party), and data that is aggregated from consumers by third-party data brokers and sold (third-party). Data broker markets in particular, which are valued at more than $200 billion worldwide, offer AI systems data inputs of vast scope and often of which the subjects of the data, the ones being processed, are blithely unaware.

The data collection surface is further enlarged by the Internet of Things (IoT). AI profiling systems ingest various types of behavioural, physiological and contextual data from a variety of smart devices in the home; connected vehicles, wearable health monitors and ambient sensing infrastructure in near real-time. The resulting picture is an aggregate that is qualitatively different from what was thought of by the lawmakers who designed data protection laws a decade or more ago.

3. Legal Frameworks Governing Data Protection

3.1 The European General Data Protection Regulation (GDPR)

It provides a comprehensive scope, a risk-based approach and considerable enforcement capabilities, making it the de facto global standard to which other frameworks are measured. A few of the provisions are directly relevant to profiling based on AI.

Article 22 gives data subjects the right to refuse being part of entirely automated decisions that have a 'significant effect' on them, with 3 enumerated exceptions. Article 13-14 impose transparency obligations, including the need to inform people of the controllers' use of automated decision-making, including profiling. The rights of erasure (article 17) and the right of objection to profiling (article 21). The principle of Data Protection by Design and Default in Article 25 laid a burden for privacy on architecture.

The limits of these provisions have been pushed by the supervisory authority enforcement. The decision of the "Irish Data Protection Commission" to fine Meta for €1.2 billion in 2023 for failing to provide sufficient documentation to build the case that they have acted in a legitimate manner in provisioning behavioral advertising

was an indicator of the regulators' appetite to challenge large tech entities. In that regard, objections raised by the French CNIL against Google and Apple for cookie consent mechanism have been an indication of increased scrutiny upon profiling infrastructure.

3.2 The California Consumer Privacy Act / California Privacy Rights Act

The CCPA (which took effect in January 2020, and was greatly amended by CPRA, also effective in January 2023) provides a leading US state-level privacy framework. The CPRA also added new protections specifically related to profiling with AI: "the right for correct inaccurate personal information, the right to be forgotten for processing of sensitive personal information, and a new California Privacy Protection Agency (CPPA) enforcement mechanism".

There are important differences in the structural approach of the CCPA/CPRA framework compared to the GDPR. It is an opt-out model, not an opt-in consent model, and thus a default setting that benefits commercial data use. "The right to opt out of the 'sale' or 'sharing' of personal information for cross-context behavioral advertising is part of the heart of the regime, but the meaning of 'sale' or 'sharing' has been challenged in cases and regulatory investigations. Importantly, the CPRA's automated decision making language is still more restricted than Article 22 GDPR and the rules to implement the CPPA are still in development".

3.3 India's Digital Personal Data Protection Act 2023

"The Digital Personal Data Protection Act, 2023" (DPDPA 2023), was adopted in August 2023, which will provide a framework for the protection of digital personal data. The Act draws upon the landmark decision of "Puttaswamy v. Union of India" (2017) in which the Supreme Court reaffirmed that the right to privacy is a fundamental right that establishes consent based architecture of the proposed Act and introduces the "Data Protection Board" as the enforcement authority. A few features stand out in connection with AI profiling.

Carrying out the processing of any data must be based on 'free, specific, informed, unconditional and unambiguous' consent and the right to withdraw consent at any time. Since there is no Indian equivalent of "controllers", "data fiduciaries" as in the UK should be making clear notices beforehand. Certain duties are linked to 'Significant Data Fiduciaries' defined by the Central Government, and would probably encompass massive AI operators. The Act, however, lacks a comparable amount of prescription on profiling and automated decision making as the GDPR does and important regulatory detail is yet to be fleshed out through subordinate legislation.

4. Core Challenges at the AI–Privacy Nexus

In the sections below, we discuss six challenge domains, in which the convergence of AI capacities and existing data protection frameworks produces key tensions. The three main jurisdictions that are being studied are the viewpoints used for each of the domains.

4.1 Algorithmic Opacity and the Right to Explanation

The 'black box' problem is at the core of the AI-privacy challenge. Predictive accuracy of contemporary deep learning systems, especially transformer language modeling systems and deep neural networks, depends on representations that are not human-interpretable. Such opacity is not a technical impediment it is a structural one that provides obstacle to the use of fundamental privacy rights.

The need of 'meaningful information' regarding the logic behind an automated decision (Recital 71 of GDPR and Article 22(2)(b) GDPR) has given rise to a doctrinal controversy that has been ongoing for quite some time. The U.S. courts have, importantly, also ruled that a proprietary risk assessment algorithm could be used in criminal sentencing, without explaining the logic behind it (Loomis v. Wisconsin 2016). In 2023 the Court of Justice of the EU in C-634/21 (SCHUFA Holding) confirmed that the processing of credit scoring is indeed considered profiling under Article 22 GDPR and thus falls under the right to explanation but what the content of this explanation should be remains contentiously debated.

The challenges are intense: meet meaningful and explainable requirements with the disclosure of model structure, data of model training, and the weights of features that controllers consider as trade secrets.

4.2 The Legal Adequacy of Consent Frameworks

In today's privacy regimes, the rule and norm that guides data processing is assembled through consent. But the consent system is usefully geared towards the world where you can identify discrete bits of data transactions. AI profiling systems work on huge collections of data, collected over long time spans and treated in ways that the subjects of the data collection could not have predicted, from which inferences the output of the system are drawn that may have nothing to do with the input of data the subjects said they consented to have collected.

The phenomenon of 'consent fatigue' also reflected by fact that people do not usually read privacy policies consequently, calls into question the normative legitimacy of consent as a mechanism. Research has consistently shown that the typical consumer would have to spend more than a quarter of a day a year reading privacy policies he or she encounters. Structurally coercive consent arrangements are bundled and "take it or leave it," especially if non-consent means lack of access to critical digital services.

GDPR's consent requirements that consent must be freely given, specific, informed and unambiguous are common sense and often undermined by "dark patterns": pre-ticked boxes, misleading interface design and consent journeys that take the users through a sequence of steps that incrementally lead to greater use of data. Guidelines on Dark Patterns 3/2022 from the EDPB and the CPPA's proposed regulations on dark patterns are regulatory responses which are enforced episodically.

4.3 Cross-Border Data Flows and Jurisdictional Fragmentation

AI profiling systems are world-wide architected. Often training, inference infrastructure and data subjects are located in multiple jurisdictions. This results in a number

of acute issues of fragmentation of jurisdiction that is, which law applies? Who is the authority that regulates? If the data processing takes place on servers in one continent, employs companies incorporated in another continent, and impacts consumers in a third continent, what will be the remedies to data subjects?

Equivalence whereby the European Commission can opine that the protection in a third country is adequate for the purposes of the GDPR has been found to be an inconstant mechanism. This was due largely to the Court of Justice's judgments on Safe Harbour (2015) and Privacy Shield (2020) being invalidated, causing disruption to EU-U.S. data flows for years to come. The EU-US Data Privacy Framework (2023) provides a new path for transatlantic data transfer, but is currently legally challenged.

India's DPDPA has a white listing approach to cross-border transfers, allowing for transfers to countries as specified by Central Government with certain restrictions on processing of children's data. Bilateral data-sharing treaties and possible data localisation will that reduce opportunities to build the global AI economy?

4.4 Profiling of Sensitive and Inferred Attributes

Certain types of personal information are sensitive and are given greater protection in the data protection regimes these are sensitive data and include race, ethnicity, health, sexual, political opinions and religious beliefs. By default, it is forbidden to process them under GDPR unless the user has given consent or there is a specific legal basis. But AI is continuously making statements on these attributes from non-sensitive input data, thereby generating a super-regulatory void.

According to a study published in Nature Human Behaviour, non-sensitive behaviours patterns in a person's Facebook 'likes' can accurately predict their sexual orientation with 88%, ethnicity with 95%, and even political affiliation with 85%. The output inference would not be considered sensitive information and the processing would not be considered privileged processing under existing arrangements as the information that was used as input data would not be considered sensitive.

This is a structural shortfall. Not the categorisation of the input data, but the content of the functional application of the inferences defines the harm of privacy. Systematic failure of legal regimes whose protection is linked to categorisation of the inputs. However, when the AI capabilities arose making the light problem severe, there were concerns raised in the purpose limitation section of the Opinion 03/2013 rendered by the Article 29 Working Party.

4.5 Children's Data in AI-Powered Environments

Children are a group of data subjects whose data is especially vulnerable. AI is used pervasively across a range of domains in the education system, social media, games and connected toys, which provides an embedded substrate for children to be profiled, beginning from infancy. AI profiling takes place across the longitudinal, with profiled data generated over a period of time, and potentially affecting life-changing decisions decades later.

The GDPR limits the use of information society services which affect children's data, where the age of consent to data processing is not yet reached, thus rendering the age limit as 13 to 16 years (according to different member states). The UK Children's Code, then, takes it a step further; child appropriate default settings, ban on profiling for commercial uses and ensuring that systems do not significantly negatively impact child wellbeing. The notice and consent obligations for under-13s continue with the US Children's Online Privacy Protection Act (COPPA), which predates the AI era.

Age verification is still a critical issue. New technologies such as AI-based age estimation on images present other privacy issues, and protection of children's privacy can paradoxically involve collecting and processing network information of a type that may otherwise be banned, such as biometric information.

4.6 AI Innovation Imperatives vs. Privacy-by-Design

A primary conflict in the regulatory landscape is between the innovation pressures behind AI and the privacy-preserving aspirations of DP law. Requirements of privacy by design and data minimization are integral to the GDPR and other new frameworks, and can contradict the data maximalism of today's AI development, which often thrives with big and richer data sets.

Technical solutions to address this tension include differential privacy, federated learning, and generation of synthetic data. These privacy-enhancing technologies (PETs) can also greatly diminish privacy risks while maintaining a significant amount of the usefulness of AI training data. However, their adoption will need not only technical investment, but also regulations that encourage, or indeed demand, their use. There is a non-uniform regulatory regime that isn't always encouraging innovation around preserving privacy.

5. Comparative Analysis of Regulatory Responses

5.1 Approaches to Automated Decision-Making

The most major difference between the three frameworks is with regards to automated decision making. At the most prescriptive end of the GDPR is Article 22 which establishes a right to restrict the making of automated decisions with significant effects, except for certain specified purposes which will involve specific safeguards such as having the right to a human review of the decision. The CCPA/CPRA does not have a similar provision, and regulations regarding automated decision-making technology are currently under development in the CPPA. India's DPDPA is equally deficient in the area of automated decisions.

In July 2024, the EU AI Act (Regulation 2024/1689) was published in the Official Journal, greatly enhancing the regulatory landscape for the use of AI in high-risk scenarios by mandating that AI systems undergo compulsory conformity assessments and comply with various human oversight and transparency rules in certain cases. This added measure fills some of the parole's unanswered questions in the GDPR definition of profiling, although there are some harmonisation issues on the interpretation of the measure with article 22 of the GDPR.

5.2 Approaches to Data Subject Rights

Rights to Access, Corrections, Deletion, and Portability are common to all three contexts. But these rights have a limited application and to a certain extent, enforceability in an AI environment. Automated decisions are included as part of the GDPR right of access and the distinction between the right to correction and the right to have all inferences deleted may be problematic in the case of probabilistic inferences.

5.3 Enforcement Architectures

This is what enforcement is referred to as the sensitive factor that distinguishes between effective protection and good design rules. Of the three enforcement mechanisms examined, the best is that of the GDPR, which is a multi-layered system comprising of national supervisory authorities with significant administrative sanctioning powers, a consistency mechanism for cross-border cases, private persons right of action and finally, representative action by civil society organisations. While some of the record fines imposed on some of the major tech platforms have been challenged, they have certainly shown its capability.

6. Case Studies

6.1 Real-Time Bidding and Online Advertising

Most of the digital advertising inventory is sold using auction-based methods known as real-time bidding (RTB). The period of time that occurs while a user views a webpage and deciding to keep browsing milliseconds is a time when data about the user is passed around to thousands of advertising tech companies including their browsing habits, inferred demographics, and web browsing profiles. This data broadcast estimated to be trillions of bid requests each day is maybe the greatest processing of personal information in history.

The Irish Data Protection Commissioner (IDPC) investigated the RTB system in 2022 and discovered several instances of GDPR violations, such as no legitimate use of the personal data broadcasted and a lack of transparency. The industry's Transparency and Consent Framework (TCF) is unlawful under the GDPR, the Belgian Data Protection Authority announced. These regulatory initiatives have continuously challenged the legal underpinnings of RTB and have ramifications for the infrastructure of AI-profiling that is built on it.

6.2 AI Credit Scoring in Financial Services

AI credit scoring systems are a good example of this kind of profiling with consequences, which is what Article 22 GDPR has been conceived to combat. The biggest credit scoring models today take hundreds or thousands of factors into account such as social network connections, smartphone usage habits and typing patterns to come up with credit risk predictions. The implications that these spellings have on generation of access to credit, housing and insurance have major repercussions for individual economic life chances.

In the case of SCHUFA Holding (C-634/21, 2023), the CJEU ruled that the automated credit scoring is in scope of Article 22 of GDPR, meaning it is subject to human involvement of the affected persons. Enforcement actions of German, French and Dutch regulators include around discriminatory credit scoring systems which exacerbate historical biases that are built into the training data. The case demonstrates that algorithmic "opacity" can intersect with discriminatory profiling and thus can create compound harms.

6.3 Children's Profiling on Social Media

In April 2023, the UK Information Commissioner's Office (ICO) investigated TikTok and determined that it was not using data about children in accordance with the UK GDPR and Children's Code and issued a fine of £12.7 million. It also found that TikTok had collected data of children under 13 without parental consent, from different data collection activities, it was used in ways incompatible with why it was collected, and it lacked sufficient default privacy protection.

This case highlights the specific risks faced in environments where AI is in use and children are clearly at stake. TikTok's core recommendation system, which is a complex AI designed to track a child's viewing habits, and generate personalized recommendations to influence their actions and future viewing patterns, is exactly the sort of profiling mechanism that is inherently dangerous when it comes to children's wellbeing and development if it is not properly managed.

7. Conclusion

Consumer profiling by AI is one of the greatest privacy concerns of today's digital age. The systems studied for this paper, operating in the fields of behaviour analytics, predictive modelling, natural language processing and social graph analysis, are building up a picture of a consumer with almost micro granularity, and often without the consumer's knowledge, consent and appropriate control.

The examined legal frameworks GDPR, CCPA/CPRA, and DPDPA represent a real success in articulating privacy rights against commercial data exploitation. Indeed, the GDPR in particular has shown how effective robust privacy legislation can be in regulating the activities of even the largest technology companies in the world through substantial enforcement actions and interpreting the GDPR by the CJEU. However, this paper's analysis shows that there are some inherent weaknesses in these frameworks that existing enforcement processes will not be able to correct.

Systematic under-regulation of AI-generated sensitive attributes compared to sensitively declared data (inference gap) is the utmost urgent reform priority. California and India have yet to solve the opacity issue either; the EU AI Act helps with it in part. The consent model, which applies to a landscape of finite data transactions, does not fit AI systems that work on data in ways that may not be sensibly foreseen when it is gathered. Jurisdictional fragmentation allows regulatory arbitrage in a big way. Addressing these challenges necessitates action at several layers: legislative reform to fill gaps in definitions; regulatory capacity development to facilitate implementation of new rules; international coordination to

address fragmentation at the regulatory level; and technical investment into privacy-enhancing technologies to make economic privacy-preserving AI possible. The other potential is that the world is devoid of proper legal regulation and AI profiling becomes pervasive, which endangers the idea of autonomy, democratic citizenship, and informed agency more broadly.

The jurisprudential tendency is positive. Councils and regulators around the world are getting more knowledgable regarding AI technologies. But the big question for lawmakers and legal academics as the legal profession navigates this steep learning curve is whether this complexity will eventually solidify into stable and workable, enforceable solutions that will keep pace with AI potential

REFERENCES

Primary Legal Sources

- General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [2016] OJ L119/1 (GDPR).
- California Consumer Privacy Act (CCPA), Cal. Civ. Code §§ 1798.100–1798.199.100 (2018, as amended by CPRA 2020).
- Digital Personal Data Protection Act 2023 (India), No. 22 of 2023, Ministry of Electronics and Information Technology.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L1689.
- Case C-634/21 OQ v. SCHUFA Holding AG [2023] ECLI:EU:C:2023:957 (CJEU, Grand Chamber).
- Case C-311/18 Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems [2020] ECLI:EU:C:2020:559 (Schrems II).
- Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 (Supreme Court of India).

Academic Literature

- Calo, R. (2014). 'Digital Market Manipulation.' George Washington Law Review, 82(4), 995–1051.
- Cohen, J.E. (2012). Configuring the Networked Self: Law, Code and the Play of Everyday Practice. Yale University Press.
- Edwards, L. and Veale, M. (2017). 'Slave to the Algorithm? Why a Right to an Explanation Is Probably Not the Remedy You Are Looking For.' Duke Law & Technology Review, 16(1), 18–84.
- Hildebrandt, M. (2008). 'Defining Profiling: A New Type of Knowledge.' In M. Hildebrandt and S. Gutwirth (eds.), Profiling the European Citizen. Springer, pp. 17–45.
- Kaminski, M.E. (2019). 'The Right to Explanation, Explained.' Berkeley Technology Law Journal, 34(1), 189–218.
- Kosinski, M., Stillwell, D. and Graepel, T. (2013). 'Private Traits and Attributes Are Predictable from Digital Records of Human Behavior.' Proceedings of the National Academy of Sciences, 110(15), 5802–5805.
- Malgieri, G. and Comandé, G. (2017). 'Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation.' International Data Privacy Law, 7(4), 243–265.
- Nissenbaum, H. (2010). Privacy in Context: Technology, Policy and the Integrity of Social Life. Stanford University Press.
- Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press.
- Solove, D.J. (2013). 'Introduction: Privacy Self-Management and the Consent Dilemma.' Harvard Law Review, 126(7), 1880–1903.
- Zarsky, T.Z. (2016). 'The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making.' Science, Technology, & Human Values, 41(1), 118–132.

Regulatory Guidance and Reports

- Article 29 Data Protection Working Party (2018). Guidelines on Automated Individual Decision-making and Profiling for the purposes of Regulation 2016/679 (WP251rev.01). European Data Protection Board.
- California Privacy Protection Agency (2023). Proposed Regulations: Automated Decisionmaking Technology. CPPA.
- European Data Protection Board (2022). Guidelines 3/2022 on Dark Patterns in Social Media Platform Interfaces. EDPB.
- Information Commissioner's Office (2023). TikTok Penalty Notice. ICO, Case Reference COM0804796.
- Irish Data Protection Commission (2023). Decision against Meta Platforms Ireland Limited. DPC, Case Reference IN-20-7-2.

1. OECD (2019). Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449..

.