KING'S College LONDON

After Third Party Tracking:
Regulating the harms of behavioural advertising through data protection

Project Report
May 2022

Authors

This report was authored by Perry Keller, Reader in Media and Information Law, King's College London with assistance from Dr. Li Yang and Dr Tom van Nuenen, Research Associates, King's College London.

Many thanks to Professor Tanya Aplin, King's College London for her comments.

Annex One was prepared by Perry Keller and Annexes Two and Three were prepared by Dr Li Yang.

1. Research project

Research Project

This is the final report for the King's College London '**After Third Party Cookies - Consumer consent and data autonomy in the globalised AdTech industry'** research project, which was funded by the Information Commissioner's Office (ICO) research grants programme.

Research Project Team

Principal Investigator:

Perry Keller, Reader in Media and Information Law, King's College London

Research Associates / 博士后研究员:

Dr. Li Yang, King's College London and

Dr Tom van Nuenen, King's College London

Methodology

Desk-based review of primary and secondary sources

Workshop discussions with invited participants

Terminology

In this study the term 'behavioural advertising' refers to the interconnected processes used to collect or infer and further process information (primarily personal data) for the purpose of personalised marketing and advertising of goods and services, including tracking, profiling and automated decision-making, targeting and attribution. Behavioural advertising relies on digital platforms and specialised intermediaries. It is also known as Adtech, programmatic advertising and surveillance advertising.

For simplicity, this Report uses basic UK data protection terminology, including 'personal data', 'processing', 'data subject' and 'data controller', as these concepts have parallel terminology in relevant data protection legislation in not only the EU, but also the United States and China. Nonetheless, even when the same terms have been adopted in the U.S. or Chinese legislation, the meanings are not identical. Direct references to U.S. or Chinese law will use the correct terms (e.g., 'consumer privacy', 'personal information').

Annexes

Annex One: United States - Consumer data protection legislation
Annex Two: China - Consumer related data protection legislation and regulations
Annex Three: China - Special Rectification Scheme for Mobile Apps (2019 – 2022)

2. Summary

- Behavioural advertising operates in similar ways across the four jurisdictions under discussion – the UK, EU, United States and China.

- Behavioural advertising has significant potential benefits and risks of harm, although the perception of these benefits and harms varies significantly with differences in cultural, social and political perspectives.

- In all four jurisdictions, behavioural advertising in the midst of major structural changes brought about by regulatory pressures as well as changes to operating systems, browsers and platform rules in relation to third party cross web and cross app tracking.

- Despite legal and policy context differences, consumer related data protection laws across the four jurisdictions all rely on notice and consent / choice frameworks as the basic mechanism for legitimising the sharing of personal data for advertising purposes.

- This key shared feature means that all four regulatory regimes face similar challenges in delivering genuinely informed and meaningful choice to consumers in complex digital environments, including behavioural advertising.

- These challenges are exceptionally important as new personalised services, devices and environments, many featuring integrated advertising, will operate on the basis of the basis of current legal and regulatory decisions regarding consumer choice and personalisation.

- While consumer data protection in the United States and China operates in distinctively different legal and policy contexts, there are clear similarities with the UK and EU in their regulatory focus on repairing the conditions and mechanisms of notice and consent / choice (‘opt ins’ and ‘opt outs’).

- Across the four jurisdictions, data protection regulators are facing the increasing problem of consumer incapacities in complex digital environments, which is evident not only in the commercial exploitation of online notice and consent / choice interfaces, but also in regulatory interventions that implicitly recognise that genuinely informed, deliberative decision making for the average consumer in these environments has become increasingly unlikely.

- Legislative, judicial and regulatory pressures, in combination with operational changes introduced by major tech platform and system providers, are now breaking down Real Time Bidding systems. The push to introduce one click online consent refusal or opt out solutions to

cross web and cross app tracking has played a major part in this growing success, empowering consumers to act on their dislike of RTB's crude and ubiquitous tracking.

- In the next behavioural advertising era, the mechanisms of data extraction, profiling and targeting will be better designed to navigate notice and consent / choice requirements and better adapted to exploit increasing consumer incapacities in complex digital environments. In this dawning era, legislative and regulatory management of online notice and consent / choice interfaces is unlikely to be a viable long-term strategy.

- Across the four jurisdictions discussed in this study, there is a broad awareness of this problem as well as an evident emergence of alternative harms based regulatory approaches to behavioural advertising, including use of principles of fairness and reasonableness, the creation of protective regimes for vulnerable groups, especially children, and the introduction of risk based regulation for artificial intelligence. Given consumer data protection law's structural commitment to notice and consent / choice frameworks, these harms based solutions will surround and overlay with rather than replace those frameworks.

- It is apparent that the future regulation of behavioural advertising harms will occur through overlapping regulatory measures that operate both inside and data protection law. To be effective, this needs to be carefully planned and coherently applied rather than developing as an ad hoc series of responses to the weaknesses of notice and consent / choice mechanisms in the face of innovations in targeted advertising.

3. Behavioural advertising – A global phenomenon

"Digital technologies have enabled firms to collect data on individuals at a hyper-granular level, tracking not just what a person purchased, for example, but also their keystroke usage, how long their mouse hovered on any particular item, and the full set of items they viewed but did not buy. As people rely on digital tools to carry out a greater portion of daily tasks, the scope of information collected also becomes increasingly vast, ranging from one's precise location and full web browsing history to one's health records and complete network of family and friends. The availability of powerful cloud storage services and automated decision-making systems, meanwhile, have allowed companies to combine this data across domains and retain and analyze it in aggregated form at an unprecedented scale—yielding stunningly detailed and comprehensive user profiles that can be used to target individuals with striking precision."[1]

[1] Remarks of FTC Chair Lina M. Khan, IAPP Global Privacy Summit 2022 Washington, D.C. 11 April, 2022 https://bit.ly/3xHPBR6

The emergence of new data protection regimes around the world is a promising sign that commercial abuses of personal data will become less prevalent. Nonetheless, the jurisdictional frontiers of these regimes are complex, giving rise to problems of extra-territorial over-extension as well as territorial non-applications. Differences in regimes present a significant risk of creating exploitable gaps between these regimes as well as a cost risk for businesses as their overlapping requirements multiply. Additionally, as the range of personalised digital services increases, some of which relying on advertising as a revenue stream, a better understanding of the inter-relationship of consumer data protection regimes will also be needed. In a pandemic and war distressed world, global cooperation and coordination regarding data protection for consumers is an undoubted challenge. Yet, without better coordination of standards and enforcement, protective regional or national calls for data localisation will continue to grow, diminishing opportunities for growth and innovation.[2]

This comparative study concerns data protection based regulation of behavioural advertising in the UK, EU, United States and China. It is a remarkable feature of behavioural advertising that its structure and methods of operation are similar across these major digital economies. That is true notwithstanding the significant differences between China's online consumer economy and those of the UK, EU and United States, which are comparatively more homogeneous and inter-connected.[3] In China, mobile apps have long been the predominant way consumers access online services, which until recently have tended to be offered through rigidly controlled walled gardens.[4] While mobile app use is steadily increasing in western economies,[5] the technical infrastructure of behavioural advertising in these countries has, until recently, relied more on browser cookies than app based identifiers, including 'software developer kits' (SDKs), [6] which are the mainstay of user tracking in China.[7]

---

[2] Yan Luo, Zhijing Yu, Vicky Liu, 'The future of data localization and cross-border transfer in China: a unified framework or a patchwork of requirements?' IAPP, 22 June 2021 https://bit.ly/3GCiGOI; Theodore Christakis, ''European Digital Sovereignty': Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy', Multidisciplinary Institute on Artificial Intelligence / Grenoble Alpes Data Institute, December 2020 https://bit.ly/3p3dkGr; Jennifer Bryant, 'CNIL is latest authority to rule Google Analytics violates the GDPR', IAPP – the Privacy Advisor, 10 February 2022 https://bit.ly/3sZnOYe

[3] Lambert Bu, Violet Chung, Nick Leung, Kevin Wei Wang, Bruce Xia, and Chenan Xia, 'The Future of Digital Innovation in China', McKinsey Digital, Oct 2021 https://mck.co/33Rie1r

[4] Xuehui Hu, Guillermo Suarez de Tangil, and Nishanth Sastry, 'Multicountry study of third party trackers from real browser histories', 2020 IEEE European Symposium on Security and Privacy (EuroS&P), 70–86 https://ieeexplore.ieee.org/document/9230391; Abby Lemert and Eleanor Runde, 'Alibaba Is Fined; Other Tech Companies Are Put on Notice' Lawfare Blog, 23 April 2021 https://bit.ly/3FKEib4; Naoki Matsuda, Alibaba and Tencent start dismantling 'walled gardens', Nikkei Asia, 17 October 2021 https://s.nikkei.com/3Knm2YU

[5] Reuben Binns, 'Tracking on the Web, Mobile and the Internet-of-Things', arXiv:2201.10831 [cs.CR], 27 January 2022 https://arxiv.org/pdf/2201.10831.pdf

[6] Kretschmer et al, Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web ACM Transactions on the Web, 15/4, November 2021 https://doi.org/10.1145/3466722; Ken Harlan, 'The truth about SDK integrations and their impact on developers', TechCrunch, 12 May, 2021 https://tcrn.ch/3rsEJlr

[7] According to a 2020 report on the security and legal compliance of the SDK published by the CAICT, an affiliate research institute of the MIIT, on average one mainstream app in the market contains about 10 SDKs, whereas for some categories of apps, the average number of third-party SDKs can be over 30. Moreover, SDK developers tend to "expand the functions of their SDKs horizontally and vertically", thereby increase the SDKs ability in accessing and combining data from different variety of apps and business contexts. According to the same report, personal information collection and use by the SDK is not only beyond awareness of ordinary individual users, but can also be a "black box" for app developers as well. See: https://bit.ly/3rzxtnG, at pp 13-14, and pp 19-21.

Behavioural advertising, which is also known as targeted or programmatic advertising or more simply as Adtech, refers to automated online advertising that targets consumers by using multiple data sources that reveal potential buying interests or preferences. Behavioural advertising is frequently distinguished from contextual advertising, in which advertising is chosen according to the context in which it is viewed rather than according to data specific to the viewing consumer. Contextual advertising has existed since the origins of advertising and continues to be a significant part of contemporary advertising. Nonetheless, with increased uses of artificial intelligence, distinctions between behavioural and contextual advertising are less clear than they once were.[8]

Behavioural and contextual advertising both exist in the same two sided advertising system: advertisers (the demand-side) and publishers (the supply-side). Behavioural advertising is, however, significantly more complicated as it relies on constant streams of data regarding millions of individuals that are used to target consumers in real time as they individually visit specific websites or use particular apps. It exists in a complex system of Customer Relationship Management technologies (CRMs), Agency Trading Desks (ATDs), Demand-Side Platforms (DSPs), Data Management Platforms (DMPs), Supply Side Platforms (SSPs), Ad Networks, Ad Exchanges, Ad Servers and other entities that ensure the smooth delivery of personalised advertising to consumers.

At the heart to this system, Real Time Bidding (RTB) ensures the instantaneous appearance of an advertisement before a specific consumer delivered from the advertiser who has outbid competitors to serve that ad through this automated, algorithmic bidding process. In this process, the individual consumer's online activities are tracked across websites and apps through volunteered and observed data,[9] which is combined with other data available in the advertising system regarding that individual, as well as algorithmic inferences relevant to that collected data, to provide a profile suitable for advertising targeting, including response attribution and re-targeting.

Behavioural advertising is explained in greater detail in numerous other sources. These include –

- Maciej Zawadziński and Michael Sweeney, Clearcode Adtech Book https://adtechbook.clearcode.cc/introduction/

- ICO, Update report into adtech and real time bidding, 20 June 2019 https://bit.ly/2Xw0gLu;

- Norwegian Consumers Council, Out of Control: How consumers are exploited by the online advertising industry, 14 January 2020, Chapters 1 and 2 https://bit.ly/3bspp1z;

[8] Kabir Ahuja, Thomas Bauer, Caroline Meder, and Oliver Gediehn, 'As the cookie crumbles, three strategies for advertisers to thrive' McKinsey. 6 April, 2022 https://mck.co/3Lba98h
[9] Ana-Maria Creţu, Federico Monti, Stefano Marrone, Xiaowen Dong, Michael Bronstein & Yves-Alexandre de Montjoye, 'Interaction data are identifiable even across long periods of time', (2022) Nature Communications, Vol 13, Article 313

- Centre for Data Ethics and Innovation, Review of online targeting: Final report and recommendations, February 2020, https://bit.ly/2MJhgLV;

- Competition and Markets Authority, 'Online platforms and digital advertising market study - Final report', 1 July 2020, Chapter Two – Overview https://bit.ly/31IclD1;

- Niklas Fourberg, Serpil Taş, Lukas Wiewiorra, Ilsa Godlovitch, Alexandre De Streel, Hervé Jacquemin, Jordan Hill, Madalina Nunu, Camille Bourguigon, Florian Jacques, Michèle Ledger and Michael Lognoul, 'The Impact of Targeted Advertising on Advertisers, Market Access and Consumer Choice', European Parliament, IMCO Committee, June 2021 https://bit.ly/3AgNK58

- Giovanni Sartor, Francesca Lagioia, Federico Galli, 'Regulating targeted and behavioural advertising in digital services: how to ensure users' informed consent', European Parliament, JURI, July 2021 https://bit.ly/3f9iTh2

Additionally, as an example of how behavioural advertising works in relation to a major online service provider, Jack Brighton, 'Fueling the AdTech Machine: Google Analytics and the Commodification of Personal Data', Information Science Journal, January 2021 https://bit.ly/3tcmhjf

For an overview of behavioural advertising and its data protection based regulation in China, see Annex Three.

In the behavioural advertising sector, a distinction is often made between first party data and third party data: First party data is the personal data created within a direct relationship between a consumer and an online service, whether website or app based, that the consumer has chosen. This first party data includes not only volunteered or observed personal data, but also any inferences made about the consumer, to the extent those inferences are sufficiently specific to be personal data.[10] Third party data refers to the personal data that is shared with or accessed by a party that is outside the first party relationship, which includes advertisers. As discussed below, the distinction between first parties and third parties is also helpful when mapping the ways in which data protection law applies to processing in this sector.

However useful conceptually, the dichotomy between first and third parties is more complicated in practice. The same personal data can be first or third party data, depending on which party is processing that data. First parties are, moreover, often also third parties in unrelated first party –

[10] Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI', 2 Columbia Business Law Review, (2019)

consumer relationships (e.g., Google via Google Analytics).[11] Additionally, affiliated businesses in the same group may be represented as part of the first party relationship or as a third party for different commercial purposes.[12] To further complicate the distinction between first and third parties, data broking also plays an essential role in the collection and flow of data in behavioural advertising systems. As one recent report states, '[a] data broker is unlikely to be the entity that initially collected the data that it makes available commercially. In fact, data may often pass through several different providers before it finds its way to a data broker. Data may be purchased for one purpose, but ultimately repurposed for another, making preserving legal protections and accountability difficult.'[13]

Within the advertising sector, data that a consumer has voluntarily made public is sometimes referred to as 'zero party data' and forms part of the business model for web scraping and other data businesses. That notion usefully illustrates the distance between data protection terms and behavioural advertising terms. Asserting that web scraped data is 'zero party data' is in essence not a claim that the data is outside the scope of 'personal data' as a matter of data protection law, but instead makes a claim that images or other personal data were voluntarily made available online to anyone with internet access may be used freely for any purpose. The circumstances in which such a claim would survive scrutiny under UK or EU data protection law are limited.[14]

There is, however, a critically important shared data protection and advertising industry understanding of the meaning of 'tracking', which in both spheres typically refers to the collection of personal data regarding a particular user's activities across different online contexts, such as websites or apps, and the further processing of that data outside the originating context.[15] It is generally considered that websites or apps that are sufficiently linked or commonly labelled are regarded as a single context, within which the collection of volunteered, observed and inferred data about users is not regarded as 'tracking'. This description of 'tracking' may appear deliberately, and even unjustifiably, narrow when looked at in relation to personalisation of digital services more generally.

---

[11] Reuben Binns, 'Tracking on the Web, Mobile and the Internet-of-Things', arXiv:2201.10831 [cs.CR], 27 January 2022 https://arxiv.org/pdf/2201.10831.pdf

[12] In research undertaken as part of this study, a check of the owners of third-party SDK listed in a popular Alibaba's app (FreshHipp) showed that half of the third parties are owned by Alibaba group (5/10) and the other 5 are respectively owned by Tencent (3/10), and XiaoMi (1/10) and Huawei (1/10). Among the five third-party SDKs listed, two are not listed on Alibaba groups's website - 友盟 and UC 开发平台. Both appear instead to be data brokerage platforms. 友盟 states on its website that it is a leading 'third party comprehensive data and smart service provider'. However, a web search indicates both were purchased by Alibaba in the past decade.

[13] Center for Democracy and Technology, Legal Loopholes and Data for Dollars Report, December 2021, page 10, et seq https://bit.ly/34UKxfK

[14] Kashmir Hill, The Secretive Company That Might End Privacy as We Know It, New York Times, 18 January 2020 https://nyti.ms/3ArI4p3; Louise Matsakis, Scraping the Web Is a Powerful Tool. Clearview AI Abused It, 25 January 2020, Wired https://www.wired.com/story/clearview-ai-scraping-web/; But see, ICO issues provisional view to fine Clearview AI Inc over £17 million, 29 November 2021 https://bit.ly/3EmUPSN; CNIL, Facial recognition: the CNIL orders CLEARVIEW AI to stop reusing photographs available on the Internet, 16 December 2021 https://bit.ly/3nEcM9f

[15] Reuben Binns, 'Tracking on the Web, Mobile and the Internet-of-Things', arXiv:2201.10831 [cs.CR], 27 January 2022 https://arxiv.org/pdf/2201.10831.pdf

Behavioural advertising frequently occurs alongside other personalised online services that are not only occurring simultaneously in the same first party relationship but are also the primary personalisation interest of the consumer. The most prevalent of these include recommender or recommendation systems,[16] which are used to structure the consumer's experience of a particular service by presenting new content based on previous choices and algorithmic inferences, such as purchase recommendations (e.g. Amazon) or video recommendations (e.g. TikTok).[17] In such circumstances the same personal data can serve several personalisation purposes, including targeted advertising involving third parties. Nonetheless, a key distinction should be made between personalisation that is necessary for a service to operate as the consumer wishes and personalised / behavioural advertising, which may be desirable to some consumers but is not technically essential to the functioning of a service. It may, of course, be financially essential to the delivery of the service.

As this report discusses, data protection law across the four jurisdictions under discussion is being progressively used to dismantle cross web and app 'tracking' for advertising purposes, yet these laws are also designed and applied to support the growth of personalised digital services. Using the term 'tracking' only for cross context data collection by unrelated businesses illustrates this tension. Tracking in this sense distinguishes one form of commercial surveillance (third party access to personal data for behavioural advertising), which is widely seen as unacceptable, from another (personalisation of first party digital services), which is seen as essential to the future of the digital economy. Within the latter sphere, the digital personalisation of human life is increasing in every direction, including innovations in digital assistants, IoT enabled vehicles and devices, and smart environments, not to mention the still uncertain potential for metaverse enabled communications and media.[18] Plainly, the degree of profiling and personalisation already occurring within these first party contexts has astonishing capacities to mould human behaviour.[19]

One of the questions that the current regulatory drive against egregious behavioural advertising practices leaves open is how data from these data saturated personalised services should legitimately flow to third parties for targeted advertising purposes, especially where those services are made affordable through the inclusion of advertising. Decisions being made now about the legitimate scope and operation of behavioural advertising ought to address that question by more than the default of 'not like this'.

---

[16] Qian Zhang, Jie Lu and Yaochu Jin, 'Artificial intelligence in recommender systems', Complex & Intelligent Systems', 2021 Vol 7; Shuai Zhang, Lina Yao, Aixin Sun, and Yi Tay. Deep Learning based Recommender System: A Survey and New Perspectives', ACM Computing Surveys, Volume 52 Issue 2020; Reshma Narayanan Kutty, Claudia Orellana-Rodriguez, Igor Brigadir, and Ernesto Diaz-Aviles, 'Personalization, Privacy, and Me', Recsyslabs Technical Report 2021 https://arxiv.org/pdf/2109.06990.pdf

[17] Ben Smith, How TikTok Reads Your Mind, New York Times, 5 December 2021 https://nyti.ms/3KsZ5DB; Helen Toner, Paul Triolo and Rogier Creemers, 'Experts Examine China's Pioneering Draft Algorithm Regulations' DigiChina, 27 August 2021 https://stanford.io/33xDyJs

[18] See, for example, Jennifer Pattison, 'Matter's Plan to Save the Smart Home' The Verge, 28 December 2021 https://bit.ly/3tOpGFc; David Pierce, How Matter became the future of the smart home, Protocol, December 8, 2021, https://www.protocol.com/matter-smart-home; Daniel Wroclawski, Matter, Explained: What the New Standard Could Mean for Your Smart Home, Consumer Reports, January 7, 2022 https://bit.ly/3rqgzYw

[19] Statement of Frances Haugen, United States Senate, Sub-Committee on Consumer Protection, Product Safety, and Data Security, October 4, 2021 https://bit.ly/3GWvhwt

4. Confrontations over benefits, harms and values

There are well recognised potential benefits and risks of harm associated with behavioural advertising, although the perception of these benefits and harms varies culturally and politically. The potential benefits include those of personalised services generally (e.g. effectiveness, efficiency and convenience) as well as providing financial support for online services.[20] The risks of harm[21] include loss of control over one's personal data (both in collection and in subsequent uses other parties), chilling effects of commercial surveillance (including uncertainties regarding links with state surveillance),[22] unjustifiable bias or discrimination in decisions affecting individuals or groups, deceptive manipulation (including targeted 'disinformation' designed to interfere in democratic decision making[23] as well as online user interfaces designed to obfuscate and impede informed consumer decision-making, widely known as 'dark patterns')[24] Significantly, these potential benefits and risks of harm are societal as well as individual, which raises questions about the suitable design of regulatory responses, including whether societal impacts be effectively addressed through individual focused rights and remedies.[25]

Beyond the incommensurable nature of these benefits and harms, whether individual or collective, they also concern entrenched, conflicting views about the future of digital economies and societies. Undoubtedly, there are many mixed opinions and uncertainty in this debate. Nonetheless, it is helpful to identify key perspectives and goals to understand the deeper significance of particular legal arguments, which are frequently technical and whose meaning is often obscure to the general public. As discussed below, the advertising sector is making changes to accommodate demands from regulators and courts for better data protection. Yet, it is fair to say that the online commercial sector

[20] HIS Markit, The Economic Value of Behavioural Targeting in Digital Advertising, IAB Europe, September 2021 https://bit.ly/3rzJF7Y; Note there is considerable disagreement as to whether behavioural advertising produces substantially more revenue than contextual advertising, see, for example, Panoptycon Foundation, Joint statement on surveillance-based advertising and the Digital Services Act, 12 January 2022 https://bit.ly/3tGYJUe

[21] Danielle Keats Citron and Daniel Solove, 'Privacy Harms', GWU Legal Studies Research Paper No. 2021-11 https://ssrn.com/abstract=3782222; International Working Group on Data Protection in Technology, Working Paper on the Risks emerging from the Tracking and Targeting Ecosystem in the Digital Advertising Market 24 April 2021 https://bit.ly/3MGd5Kt

[22] Carey Shenkman, Sharon Bradford Franklin, Greg Nojeim and Dhanaraj Thakur, Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers, Center for Democracy and Technology, 9 December 2021 https://bit.ly/33rUTU

[23] Karen Hao, 'How Facebook got addicted to spreading misinformation' Technology Review, 11 March 2021 https://bit.ly/3rPwgtl; Michael Toth, Nataliia Bielova, Vincent Roca, 'On dark patterns and manipulation of website publishers by CMPs', PETS 2022 - 22nd Privacy Enhancing Technologies Symposium, Jul 2022 hal-03577024 https://bit.ly/37PTjh7

[24] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 'Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence', 2020 https://arxiv.org/pdf/2001.02479.pdf

[25] Electronic Frontier Foundation (EFF) and ACLU California Action Comments, California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments – Part One, 8 November 2021, https://bit.ly/3KlOKcQ; FTC Commissioner Rebecca Kelly Slaughter, Disputing the Dogmas of Surveillance Advertising, National Advertising Division Keynote 2021, 1 October, 2021 https://bit.ly/3ty01AK

in the UK, EU and the United States remains largely committed to the idea that reformed behavioural advertising is a legitimate and necessary feature of the digital economy.[26]

In general terms, this means –

- Further personalisation of digital services is essential to economic growth
- The online public sphere should be free from the excessive intrusion of private rights.
- Consumers should be free to choose the goods and services they want, including personalised advertising with the degree of data protection they prefer.
- Data protection based regulation of advertising should not be over-inclusive and restrict the development of other personalised digital services.

In practical terms, this means -

- Rescuing viable third party access to personal data for behavioural advertising purposes from encroaching restrictions, including intermediated anonymity or pseudonymity
- Defending multi-purpose processing in first party relationships, including for internal marketing and advertising purposes
- Integrating targeted advertising into new personalised services, devices and environments
- Ensuring the lawfulness of exchanging personal data for services
- Avoiding compulsory provision of free online services based on contextual advertising

For opponents of behavioural advertising, which clearly includes most privacy activist organisation in the UK, EU and the United States, targeted third party advertising is inherently illegitimate and irredeemable.[27]

In general terms this means -

[26] HIS Markit, The Economic Value of Behavioural Targeting in Digital Advertising, IAB Europe, September 2021 https://bit.ly/3rzJF7Y; Graham Mudd, 'Privacy-Enhancing Technologies and Building for the Future' Meta / Facebook, 11 August 2021 https://bit.ly/3sbKepV

[27] Mariano Delli Santi, Our Fight Against Adtech Gets Bigger, Open Rights Group, 11 December 2020. https://bit.ly/38zpQoZ; Justin Sherman, Data Brokerage and Threats to U.S. Privacy and Security, Written Testimony before U.S. Senate Committee on Finance, 7 December 2021 https://bit.ly/3Knq5V9; FTC Commissioner Rebecca Kelly Slaughter, Disputing the Dogmas of Surveillance Advertising, National Advertising Division Keynote 2021, 1 October, 2021 https://bit.ly/3ty01AK

- Individuals should enjoy genuine, meaningful agency in relation to their personal information.

- The growing commodification of human life should be rolled back.

- Law should be used aggressively to force the re-construction of essential privacy lost to 'surveillance capitalism'.

In practical terms, this means -

- Ending tracking, profiling and targeting for third party advertising purposes and dismantling Real Time Bidding systems

- Restricting profiling and targeting for internal first party marketing and advertising purposes

- Ensuring that all online advertising is contextual and not behavioural

- Limiting personalisation of digital services to circumstances where it is essential to provide a service freely chosen by informed consumers

In China, there is a comparable debate occurring over the future of behavioural advertising. The Chinese online consumer services sector is deeply invested in behavioural advertising and, while the value of personal autonomy is less significant, economic growth arguments carry considerable weight. Unsurprisingly, the civil society based, privacy activist organisations that are central to this debate in Europe and the United States are virtually non-existent in China.[28] On the other hand, the Chinese government's recent and extensive crackdown on market manipulation by major tech companies and its new policy commitment to 'common prosperity' does mean that economic growth arguments are no longer as persuasive as they were in the past.[29] There are, consequently, policy concerns and regulatory measures in China that look similar to those occurring in the UK, EU and the United States. Strengthening protections for online consumers against unfair treatment or data security risks in China is not, however, grounded in justiciable fundamental rights or in personal autonomy as a

[28] Han Zhu, and Jun Lu, 'The Crackdown on Rights-Advocacy NGOs in Xi's China: Politicizing the Law and Legalizing the Repression' Journal of Contemporary China (Forthcoming 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3887239; Note that official China Consumer Associations (CCA) have played a limited role in promoting data protection, although they have engaged in some data protection related representative action litigation 江苏消保委对百度"涉侵犯消费者隐私"撤诉：APP 整改到位, The Paper.CN, 14 March 2018 https://www.thepaper.cn/newsDetail_forward_2028107; 重庆首例消费者个人信息保护民事公益诉讼案调解结案, PKULaw.com, 23 September 2021 https://bit.ly/33OCDUQ.

[29] Vincent Ni, TechScape: Xi Jinping's 'Little Red Book' of tech regulation could lead the way, The Guardian, 3 November 2021 https://bit.ly/353zqkQ; Brian Liu, Raquel Leslie, China's Tech Crackdown: A Year-in-Review, Lawfare Blog, 7 January 2022 https://bit.ly/3KnrHOI

significant public policy value. Yet, to some extent, those differences enhance rather than detract from the value of comparisons with behavioural advertising regulation in China. With parallel consumer protection aims, regulatory policy in China is ultimately less concerned than its western counterparts with achieving data protection through the exercise of right-holder personal autonomy and more open to direct intervention in consumer markets to achieve adequate levels of protection from identified harms. Regulatory interventions in China, such as the Special Rectification Scheme for Mobile Apps, are thus worth close attention.[30]

5. The end of third party cross web and cross app tracking?

In recent years, third party access to personal data has provided a focus for radically as well as mixed views on behavioural advertising. Without doubt, regulators and privacy activist organisations have long standing concerns regarding first party data collection for targeted marketing and advertising purposes.[31] It is, however, their facilitation of third party data access and tracking mechanisms that have become synonymous with Real Time Bidding (RTB) systems, in which personal data flows continually and often seamlessly between numerous parties who are well outside the knowledge or intentions of consumers. Indeed, in relation to EU data protection law, third party tracking for behavioural advertising purposes has been identified as being unlawful in multiple aspects.[32] This disregard of data protection rules includes the manipulation of online consumers through deceptive notice and consent interfaces,[33] as well as the use of concealed tracking practices such as 'fingerprinting'.[34]

---

[30] See, Annex Three

[31] CNIL, Cookies: financial penalty of 35 million euros imposed on the company Amazon Europe Core, 10 December 2020 https://bit.ly/35tjQw0 ; CNIL, Cookies: financial penalties of 60 million euros against the company GOOGLE LLC and of 40 million euros against the company Google Ireland Limited, 10 December 2020 https://bit.ly/2LK3FU3; CNIL, Cookies: the CNIL fines GOOGLE a total of 150 million euros and Facebook 60 million euros for non-compliance with French legislation, 6 January 2022 https://bit.ly/3JRn7YR; *Johnny Ryan v. IAB Tech Lab*, Hamburg District Court 2021 - Statement of case https://bit.ly/3Kqm3eH: None of Your Business NOYB, NOYB files complaints against Apple's tracking code "IDFA", 16 November 2020 https://bit.ly/3GR8By4; Robert Channick, 'Facebook privacy settlement approved: Nearly 1.6 million Illinois users will 'expeditiously' get at least $345', Chicago Tribune, 26 February 2021 https://bit.ly/3KpohuU

[32] Michael Veale and Frederik Zuiderveen Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' [2021] *German Law Journal* https://osf.io/preprints/socarxiv/wg8fq/

[33] ICO - Adtech Phase 2: Key findings https://bit.ly/35CGCii; NOYB, NOYB aims to end "cookie banner terror" and issues more than 500 GDPR complaints, May 31, 2021 https://bit.ly/3tel6Qo; EDPB, EDPB establishes cookie banner taskforce, 27 Sept 2021 https://bit.ly/31HrX9F; (Belgium) Autorité de protection des données (APD), Complaint relating to Transparency & Consent Framework, Case number: DOS-2019-01377, 2 February 2022 https://bit.ly/3JuvMiJ

[34] Pierre Laperdrix, Nataliia Bielova, Benoit Baudry, and Gildas Avoine. 2020. Browser Fingerprinting: A survey. ACM Trans. Web 14, 2 (2020). DOI: https://doi.org/10.1145/3386040; Celestin Matte, Nataliia Bielova and Cristiana Santos, 'Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework', arXiv:1911.09964, February 2020 https://arxiv.org/pdf/1911.09964.pdf; CNIL, 'Alternatives to third-party cookies: what consequences regarding consent?' 23 November 2021 https://bit.ly/3y58FJb; For China, see, "Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations." (App 违法违规收集使用个人信息行为认定方法), http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm; "Notice of the Ministry of Industry and Information Technology on launching special rectification work for APP infringing on the rights and interests of users." (工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知) http://www.gov.cn/fuwu/2019-11/07/content_5449660.htm

Across all four jurisdictions under discussion, there have been a cascade of legal and regulatory measures intended to limit third party cross web and cross app tracking of personal data for advertising purposes. New legislation as well as regulatory action has put significant pressure not only on the use of third party browser cookies, but also on mobile app based third party access to data. In China, the latter form of tracking has been an acute regulatory concern, given the importance of mobile apps in the country's digital consumer economy.[35] The impact of these varied legal and regulatory efforts should, however, not be overstated.[36] As the Chinese mobile apps regulatory experience illustrates, without technical resources and assertive enforcement policies, the influence of data protection based regulation on behavioural advertising is often limited.[37].

Major legislative and regulatory developments across the four jurisdictions are summarised here-

- European Union: Building on the existing rules of the General Data Protection Regulation (GDPR)[38] and the ePrivacy Directive,[39] complaints to national Data Protection Authorities have spurred major regulatory investigations, while new legislative restrictions on behavioural advertising have appeared in the new Digital Services Act (DSA)[40] and are likely in the proposed ePrivacy Regulation.[41]

- United Kingdom: Following Brexit, the UK has maintained its EU derived data protection laws, but has set out possible routes towards divergence, including modifications to user rights regarding automated decision making.[42]

[35] See Annex Three.
[36] Johnny Ryan and Adam Toner, Europe's Enforcement Paralysis, Irish Council for Civil Liberties, September 2021 https://bit.ly/3rnQtpc; Michael Kretschmer, Jan Pennekamp, Klause Wehrle, 'Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web', ACM Transactions on the Web, 2021 Vol.15 / 4 https://dl.acm.org/doi/10.1145/3466722
[37] 'APP Special Governance Report on the Collection and Use of Personal Information in Violations of Laws and Regulations (2019)'《APP 违法违规收集使用个人信息专项治理报告（2019）》, released in May 2020, http://www.cac.gov.cn/2020-05/26/c_1592036763304447.htm, at p 24. See more discussions in Annex Three.
[38] General Data Protection Regulation - Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/4/6/EC https://gdpr-info.eu
[39] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic (ePrivacy Directive) https://bit.ly/3fIdX2J
[40] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final, 15 December 2020 https://bit.ly/33Ptpr6; The European Council and Parliament reached provisional agreement on the final text of the Digital Services Act on 22 April 2022, which includes prohibitions regarding the targeting of children's personal data or the targeting of 'special category' personal data (such as political opinion, sexual orientation, race and health data) for advertising purposes as well as prohibitions on the use of deceptive techniques to influence user behaviour ('dark patterns'). https://bit.ly/38iAK4S
[41] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD) https://bit.ly/3qN1gdG
[42] Data: A New Direction, Consultation 2021 https://bit.ly/3ELgTHz

- United States: [See Annex One] New consumer privacy legislation at the state level has dramatically changed the data protection landscape in the United States, most notably the California Consumer Privacy Act (CCPA 2018 as amended by the California Privacy Rights Acct 2020),[43] while new enforcement policies have invigorated Federal Trade Commission enforcement against deceptive privacy policies.[44] State level governments have acted on equivalent powers.[45] Where private rights of action exist (limited in U.S. consumer privacy legislation), privacy activism has driven class action litigation;[46]

- China: [See Annexes Two and Three] Regulatory intervention by data protection authorities, based on pre-existing laws and regulations, importantly including the 2016 Cybersecurity Law (See Annex2), is now strengthened by China's first comprehensive national data protection law – the 2021 Personal Information Protection Law (PIPL).[47]

Equally if not more significant than these regulatory and litigation pressures on the advertising sector, major tech companies responsible for operating systems, browsers and platforms are also driving a transformation in third party data access practices -

- In January 2020, Google announced that it would block third party tracking cookies from using its Chrome browser (delayed to 2023),[48] following earlier elimination of these cookies from the Firefox and Safari browsers.[49] Google has also announced plans to enhance user control over third party tracking on Android devices by 2025;[50]

- Since that announcement, Apple expanded its privacy measures, including updates to its operating systems (iOS) that have significantly reduced, but certainly not eliminated, third party access for advertising purposes;[51]

[43] California Consumer Privacy Act 2018 (as amended by the California Privacy Rights Act 2020) https://bit.ly/3Afmq7j
[44] Federal Trade Commission, Division of Advertising Practices https://bit.ly/3GPxJED
[45] Adi Robertson, Google sued by DC and three states for 'deceptive' Android location tracking, 24 January 2022, The Verge https://bit.ly/3rW82hx
[46] Woodrow Hartzog, 'BIPA: The Most Important Biometric Privacy Law in the US?' in Regulating Biometrics: Global Approaches and Urgent Questions, ed. Amba Kak (AI Now 2020) https://bit.ly/3GWxLup
[47] Personal Information Protection Law, translation available at DigiChina, Stanford Cyber Policy Center: https://stanford.io/3fHLV7H
[48] Vinay Goel, 'An updated timeline for Privacy Sandbox milestones', Google, 24 June 2021 https://bit.ly/3LBmwer
[49] Third-party cookies and Firefox tracking protection, Mozilla, https://mzl.la/3oPQ26I; Manage cookies and website data in Safari on Mac, Apple https://apple.co/3HMuNdn
[50] Antony Chavez, 'Introducing the Privacy Sandbox on Android', Google, 16 February 2022 https://bit.ly/3vaNgMX; Daisuke Wakabayashi, 'Google Plans Privacy Changes, but Promises to Not Be Disruptive' New York Times, 16 February 2022
[51] If an app asks to track your activity, Apple, 28 April 2021 https://apple.co/3LztbG5; Patrick McGee, 'Apple reaches quiet truce over iPhone privacy changes', Financial Times, 8 December 2021

- Other major consumer service providers, such as Facebook[52] and Alibaba Taobao[53], have also introduces new business practices that restrict direct third party access to their vast first party personal data resources.

Additionally, online consumers have access to a growing range of privacy tools, including web browsers with built-in cookie blockers, tracking and advertising blocking software and incognito browsers, which are used by over 40 percent of internet users globally.[54]

The combination of governmental and industry restrictions and consumer privacy choices is undoubtedly causing a major restructuring in the mechanics of third party access to first party data for behavioural advertising purposes.[55] While the brunt of these changes is being felt by businesses lacking major first party personal data resources, the close connection and mutability of third and first party roles in online advertising means the entire online consumer services sector is caught up in this transformation.[56] Within the advertising sector, first party data has been identified as the key resource needed to prosper as behavioural advertising adapts to the loss of significant direct third party access.[57] This has put major online consumer platforms in a commanding position as the market levelling effects of direct third party access to their data resources decline further.[58] As discussed below, innovation in the use of first party data to produce data protection compliant forms of targeted advertising is widely seen as the future of behavioural advertising.

6. Consumer data protection law – Implicit versus express consent

The current focus on third party data tracking in all four jurisdictions under discussion demonstrates more than technical and commercial similarities in the operation of adtech or shared governmental

[52] Meta, What Are Privacy-Enhancing Technologies (PETs) and How Will They Apply to Ads? 11 August, 2021 https://bit.ly/3Mw8gmT; Graham Mudd, 'Removing Certain Ad Targeting Options and Expanding Our Ad Controls' Facebook, 9 November 2021 https://bit.ly/3GLZCP1

[53] 京东、淘宝"数据断供"：捍卫信息保护还是加剧平台垄断, Sina Finance, 11 August 2021 https://finance.sina.com.cn/chanjing/gsnews/2021-08-11/doc-ikqciyzm0862010.shtml

[54] Venky Anant, Lisa Donchak, James Kaplan, and Henning Soller, 'The consumer-data opportunity and the privacy imperative' McKinsey, April 27, 2020 https://mck.co/38nKuuR

[55] Marc Brodherson, Adam Broitman, Craig Macdonald, and Simon Royaux, 'The demise of third-party cookies and identifier', McKinsey Marketing and Sales, 12 April, 2021 https://mck.co/3IokbkG; Allison Schiff, 'Why 2021 was the Year Of Consent For Digital Media', AdExchanger, 28 December 2021 https://bit.ly/3AdNgwh

[56] Kate Conger and Brian X. Chen, 'A Change by Apple Is Tormenting Internet Companies, Especially Meta', New York Times, 3 February, 2022

[57] Simona Abis, Mehmet Canayaz, Ilja Kantorovitch, Roxana Mihet, Huan Tang, 'Privacy Laws and Value of Personal Data' Swiss Finance Institute Research Paper No. 21-92, January 2022 https://bit.ly/3BmBAIr; Brian X. Chen and Daisuke Wakabayashi, 'You're Still Being Tracked on the Internet, Just in a Different Way' New York Times, 6 April 2022

[58] Competition and data protection in digital markets: a joint statement between the CMA and the ICO, 19 May 2021 https://bit.ly/3nKpwLw; CMA to have key oversight role over Google's planned removal of third-party cookies - 11 June 2021 https://bit.ly/3Ih2ZgU; CMA investigation of Facebook's use of ad data https://bit.ly/3IlQ7WV; EU - Commission opens investigation into possible anticompetitive conduct by Google in the online advertising technology sector, 22 June 2021 https://bit.ly/3qJoyAQ; FTC, 'FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate', 19 August 2021 https://bit.ly/3AgO4AE

policy concerns. It also reflects important similarities in their data protection laws, which make third party access the weakest link in behavioural advertising information ecosystem. Indeed, in relation to consumer data processing, the similarities in their applicable data protection rules are as significant as their distinctive differences in legal contexts and policy environments. These core similarities enable a close comparison of 'consumer data protection law'[59] across the four jurisdictions in relation to behavioural advertising.

Without doubt, the underlying legal and policy differences between the four jurisdictions are also striking. As noted above, fundamental rights to privacy and the protection of personal data, which are essential to the interpretation and application of data protection law in the EU, have no direct counterparts in the United States or China, especially in relations between private parties.[60] That difference is hugely important in the practicalities of how data protection law is interpreted and applied, which has made the wider EU digital rights model increasingly distinctive.[61] On the other hand, while the United States and China may be alike in not recognising a justiciable constitutional right to privacy in online consumer contexts, the impact of divergent political and legal principles regarding security and liberty in these countries is of course vastly different.[62]

Consequently, differences in the design and interpretation of data protection legislation are readily apparent when comparing these four jurisdictions. The GDPR and the PIPL are statements of

[59] For the purposes of this study, 'consumer data protection law' as a comparative analytical concept refers to the application of data protection law in relation to consumer services, regardless of whether the applicable rules are found in comprehensive data protection legislation or specific consumer privacy legislation. On the close connection between EU data protection rights and consumer rights, see Opinion of Advocate General Richard De La Tour, Case C-319/20 *Facebook Ireland Limited V Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, 2 December 2021, para 83 https://bit.ly/33Gu91T**;** Mateja Durovic and Franciszek Lech, 'A Consumer Law Perspective on the Commercialization of Data', European Review of Private Law 5-2021

[60] Data protection law in the UK and the EU is indirectly subject to the European Convention on Human Rights (Article 8) and EU data protection law is also directly grounded in the EU Charter of Fundamental Rights (Article 7 and 8). Unlike these European fundamental rights instruments, the United States Constitution concerns federal and state government actions and does not directly govern the actions of private parties. The Fourth Amendment restricts the search and seizure powers of the state, including electronic data collection and further processing for surveillance purposes. However, there is no positive Constitutional duty for federal or state governments to legislate to protect citizens from the privacy invasive acts of other private parties. China's Constitution contains protections of fundamental rights, however these are non-justicable and find their meaning through ordinary legislation and regulation.

[61] Irion, Burri, Kolk and Milan, 'Governing "European values" inside data flows: interdisciplinary perspectives', (2021) Internet Policy Review 10.3

[62] Donald Clarke, 'Order and Law in China', GWU Legal Studies Research Paper No. 2020-52, GWU Law School Public Law Research Paper No. 2020-52, (25 August, 2020) https://bit.ly/3tGICG9; Zhang, Taisu and Ginsburg, Tom, 'Legality in Contemporary Chinese Politics' (Virginia Journal of International Law, Forthcoming https://ssrn.com/abstract=3250948; Rebecca Arcesati, 'Lofty Principles, Conflicting Incentives - An analysis of AI ethics and governance in China', Merics China Monitor, June 2021 https://bit.ly/3GPNfRK; Mary Gallagher and Blake Miller, Who Not What: The Logic of China's Information Control Strategy', *China Quarterly,* June 2021 https://bit.ly/3fGrWGn; On the notable differences between European and American legal conceptions of privacy in public spaces compare *Shulman v. Group W Productions, Inc.,* 955 P.2d 469 (1998), Supreme Court of California https://bit.ly/3AhhD53 or, *American Civil Liberties Union v. Alvarez,* 10-CV-05235 (2016) United States Court of Appeals for the Seventh Circuit https://bit.ly/2N6MeKK with *Dupate v. Latvia* (Application no. 18068/11, 19 November 2020) ECtHR http://hudoc.echr.coe.int/eng?i=001-206155 ; On the U.S. legal perspective on the public nature of information disclosed to a third party, see Peter Ormerod and Lawrence Trautman, 'A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age', 28 Albany Law Journal of Science and Technology https://ssrn.com/abstract=3005714

principles and broadly stated rules, although their similarly teleological modes of interpretation are shaped by the significant differences in teleologies – UK and EU fundamental rights based interpretation versus China's policy based approach to legal interpretation. In contrast, U.S. state consumer privacy laws, such as the CCPA, contain a multiplicity of often detailed rules, which tend to be interpreted more literally than the purposively. Additionally, in the United States, data processing abuses have driven privacy activist and general public demands for consumer privacy reforms, including recently enacted legislative provisions that explicitly address third party tracking in relation to behavioural advertising.

Nonetheless, despite these various differences, in the sphere of consumer data protection, the core legal frameworks across the four jurisdictions are conceptually and practically similar, reflecting a shared model for consumer transactions and shared textual origins for their data protection laws. The historic importance of informed consent in legitimising information collection form consumers in pre-internet transactions has been carried forward into the prominence of 'notice and consent / choice', whether explicit or implied, as a basis for lawful processing of personal data in online consumer data protection contexts. Consequently, data protection law has imported consumer law's embedded problems in finding effective solutions to the vulnerability of consumer consent and choice transaction models to unfair and deceptive practices.[63] Second, all four data protection regimes have a shared ancestry in what are known, particularly in the United States, as the Fair Information Practice Principles (FIPPs).[64] Consequently, their common reliance on notice and consent or choice rules are modified to varying extents by over-arching protective principles, such as purpose limitation and data minimisation. Although not explicit FIPPs principles, fairness or reasonable expectation principles also have potentially significant on how consent operates.

Structural similarities do not, of course, mean identical consumer data protection rules –

- **EU**: Mandatory transparency (notice) is a core principle of the GDPR and all EU privacy legislation;[65] Consent, which is a basis for lawful processing under GDPR Articles 6 and Article 9 (explicit consent for special category personal data), can arguably be substituted in relation to processing for behavioural advertising purposes with the possibility of lawfulness where necessary for the performance of a contract[66] or, also arguably, where the legitimate interests of the data controller are necessary and not disproportionate to

[63] Mateja Durovic and Franciszek Lech, 'A Consumer Law Perspective on the Commercialization of Data', European Review of Private Law 5-2021
[64] Woodrow Hartzog, 'The Inadequate, Invaluable Fair Information Practices 76 Maryland Law Review 952 (2017) https://ssrn.com/abstract=3017312
[65] GDPR, Articles 5, 12-15.
[66] EDPB - Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, para 52-54 https://bit.ly/3r43GTV: EDPB - Guidelines 8/2020 on the targeting of social media users, Version 2.0, 13 April 2021, paras 56-57 https://bit.ly/3neiUEW; but see, Data Protection Commission (Ireland), *In the matter of LB (through NOYB) v Facebook Ireland Limited*, DPC Case Reference: IN-18-5-5, 6 October 2021 https://bit.ly/3zJwkh3

the rights and interests of the data subject;[67] the validity of notice as well as consent and its potential alternatives are subject to the modulating effects of the fairness, purpose limitation, data minimisation and other principles;[68] additionally, the ePrivacy Directive, which protects against unauthorised access to information transmitted through electronic communication systems or information stored on electronic devices, requires a notice and consent interface (e.g., cookie banners or app notifications) to allow such access in consumer contexts.[69]

- **UK**: The rules are currently the same as those of the EU, although the UK has proposed, among other more limited solutions, eliminating cookie banners or popups as a notice and consent mechanism.[70]

- **USA:** [See Annex One] In the U.S. divided data protection system, consumer data protection rests at the federal level on the Federal Trade Commission's regulatory powers regarding unfair or deceptive acts or practices by businesses, which includes commercial 'notice and consent' based uses of consumer personal data, including violations of other sector specific federal laws, such as the Children's Online Privacy Protection Act; in the absence of federal consumer data privacy legislation, U.S. state governments have begun to enact laws to cover this gap (e.g., California CCPA 2018 as amended in 2020 by the California Privacy Rights Act, followed by the similar Virginia Consumer Data Protection Act 2021,[71] Colorado Privacy Act 2021[72] and the Utah Consumer Privacy Act 2022 [73]), which include core notice and consent / choice rules as well as modulation of notice and consent or choice through principles of purpose limitation and data minimisation; the Illinois Biometric Information Privacy Act 2008 is nationally significant as it includes a private right of action that has enabled major class action claims based on violations of its informed consent provisions.[74]

---

[67] GDPR Recital 47 - Overriding Legitimate Interest - … 'The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest'; Article 29 Data Protection Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, April 2014, Scenario 2 https://bit.ly/3r75MlQ; Article 29 Working Party Overview of results of public consultation on Opinion on legitimate interests of the data controller (Opinion 06/2014) https://bit.ly/3q9GYdM; and, Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6 February 2018, p.15 https://bit.ly/3ncbqCf

[68] GDPR, Article 5 - fairness, purpose limitation and data minimisation principles

[69] Eprivacy Directve, Article 5(3)

[70] UK Government Policy Paper: Data: A new direction, 10 September 2021 https://bit.ly/3pv5MNH; See also, Privacy and Electronic Communications (EC Directive) Regulations 2003 https://bit.ly/3GYTnHm

[71] Virginia Consumer Data Protection Act 2021 https://bit.ly/3gOOqpf

[72] Colorado Privacy Act 2021 https://bit.ly/3GOL4gx

[73] Utah Consumer Privacy Act 2022 https://bit.ly/3rZvyKh; On demands for higher standards, see, Consumer Report, Privacy Rights Clearinghouse, EFF, EPIC etc, Letter to Utah House of Representatives, 2 March 2022 https://bit.ly/3OOv0Rd

[74] See, for example, *McDonald v. Symphony Bronzeville Park*, Illinois Supreme Court, 2022 IL 126511 https://bit.ly/3HWnyjd; *Gonzalez v. Richelieu Foods*, U.S. District Court, Case No. 1:20-cv-04354, 24 January 2022 https://bit.ly/3LG0U0M; *In re Clearview AI, Inc., Consumer Privacy Litigation*, United States District Court for the Northern District of Illinois Eastern Division, Case No. 21-cv-0135, 14 February 2022 https://bit.ly/3t8qivB

- **China:** [See Annex Two] Following several years of gradual legislative and regulatory development regarding data protection, China's national data protection system is now crowned by the comprehensive Personal Information Protection Law 2021, which provides, in consumer contexts, for mandatory notice in combination with consent or, alternatively, necessity to conclude or fulfil a contract, or prior lawful public disclosure as a basis for lawful processing; additionally, the operation of these bases for lawfulness can potentially be modulated through principles equivalent to fairness, purpose limitation and data minimisation principles.

In relation to notice and consent / choice in consumer contexts, there is a notable dissimilarity between the UK, EU and China legislation as compared to the new U.S. state level consumer privacy laws. The former all require, where applicable, adequate notice and positive consumer consent before processing of personal data (an express opt in). In contrast, U.S. state consumer privacy laws require adequate notice and consumer acceptance (an implicit opt in).[75] This basic difference reflects the resistance of U.S. lawmakers to follow the gradual European shift since the 1970's away from implicit consent to data processing towards ever more demanding requirements for positive acts of express consent before processing commences. More recent U.S. solutions, such as those of the California Consumer Privacy Act, have been to create various rights to positive opt outs regarding, for example, the sharing of data or the use of sensitive data. These positive opt out rights are, in principle, comparable to rights to withdraw consent or object to processing in UK, EU and China data protection laws. In practice, however, the UK, EU and China positive opt in rights and the United States opt out rights can look and work in almost identical ways in online interfaces, being presented to the consumer through website or app interfaces at the moment before processing of the personal data starts.

The observant shopkeeper paradigm

The connection between consumer data protection and consumer protections in transactions for goods and services is only indirect. Using consumer personal data for advertising purposes is typically contingent to a primary transaction for the provision of goods and services (although there is the contested possibility of contractually trading access to personal data in exchange for goods or services).[76] This contingent interest of the goods or services provider in collecting personal data to facilitate targeted advertising does, however, have its own historic claims to legitimacy. In the pre-digital era, shopkeepers acquired, observed, and inferred knowledge of their customers' purchasing preferences and, among other things, could use that knowledge to market their wares to those

[75] See Annex One; U.S. privacy advocacy organisations have pressed the California government to introduce a requirement for express opt in consent in its CCPA regulatory rule making, California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments, https://cppa.ca.gov/regulations/

[76] Data Protection Commission (Ireland), In the matter of LB (through NOYB) v Facebook Ireland Limited, DPC Case Reference: IN-18-5-5, 6 October 2021 https://bit.ly/3zJwkh3

customers. Whether customers appreciated or discouraged the shopkeeper's use of this accumulated knowledge for that purpose would naturally vary. Certainly, in some circumstances, personalised service would be a demanding customer's expectation. In any event, this everyday fact of life in public spaces was based on implicit customer knowledge and consent, given that observing and inferring are instinctive human mental activities.

This historic legitimacy was both situational and bounded. The sharing of acquired, observed and inferred consumer preferences with third parties could, for example, conflict with a customer's reasonable expectations of privacy, depending on its extent and the circumstances. Additionally, where the retail relationship was based on a single individual or small establishment selling goods or services, there was the possibility of a mutuality of knowledge and trust, which would also affect norms of disclosure and confidentiality. Undoubtedly, in different societies there were also different common understandings regarding appropriate uses of personal data within that relationship and to what extent duties of confidentiality arose.

When observation and profiling of consumers is transposed to contemporary online contexts, settled understandings about implicit customer notice and consent and the legitimacy of observations and inferences about customer preferences inevitably become uncertain and contentious. Where personal data directly disclosed to a first party retailer is combined with personal data acquired through tracking the data subject's activities across other online services for targeted advertising purposes, the break with past practices is obvious. Yet, some of the historic legitimacy of shopkeeper observation and inferences has undoubtedly washed through into the ways in which data protection laws privilege first party relationship data processing as compared to third party tracking, which is under intense regulatory pressure.[77] 'Notice and consent' mechanisms in consumer data protection law can thus be understood as a formalisation of pre-existing legal and social norms about information collection by retailers (an 'observant shopkeeper paradigm') rather than merely a mechanical application of consumer purchasing norms to data processing.

7. Notice and consent / choice and the incapacitated consumer

Research for this study has shown that this is a significant moment in the global development of consumer data protection law. In relation to behavioural advertising, critical questions regarding any direct third party access to personal data collected in first party consumer relationships as well as the appropriate limits for first party data processing for advertising purposes are at the forefront of data protection law making and enforcement. This regulatory moment, moreover, has a wider significance for the development of personalised consumer services, devices and environments. In settling questions about the appropriate scope for behavioural advertising, the solutions will inevitably spill into the rules that the legitimate behavioural surveillance that enables those other personalisation

[77] Brian X. Chen and Daisuke Wakabayashi, 'You're Still Being Tracked on the Internet, Just in a Different Way' New York Times, 6 April 2022

purposes. To complicate matters further, where advertising is used to support the affordability of new personalised services, the rules governing the flow of personalised data from a consumer device or service to targeted adverting will be critically important. Where a multiplicity of linked personalised systems trade data, the risk of seamless, ubiquitous commercial surveillance is acute.

There is, however, a seemingly irresolvable problem within the current adjustment of the governing rules and commercial practices that will determine the scope and operation of legitimate behavioural advertising in the future. It is widely recognised that consumers do not have the capacity to understand and control the uses of their personal data in complex online environments.[78] This can be described as three linked incapacities: first, incapacities in navigating the interfaces of online consumer services that provide data processing options;[79] second, incapacities in understanding the consequences of personal data processing choices in those contexts, especially regarding the personalisation of services;[80] and third, an incapacity to understand and exercise data protection rights effectively in those contexts.[81] Information overloads and decision overloads are exacerbated by the limited technical knowledge of the average consumer. Additionally, the collective or societal impact of individual choices is hidden in the innumerable complexities of millions of daily choices about data sharing and the specific consequences for individuals.[82]

These incapacities stem directly or indirectly from the 'notice and consent' model of consumer data protection, which as noted has been adopted across the four jurisdictions. In their varied forms, notice and consent / choice rights rest on the assumption that individual choice about personal data sharing is essential to ensuring personal autonomy and empowerment, even in complicated online consumer environments. Plainly, loading responsibility on to individuals for data protection choices in these environments will often fall short of any notion of informational self determination.[83] While not irrational

[78] World Economic Forum, 'Redesigning Data Privacy: Reimagining Notice & Consent for human-technology interaction', White Paper, July 2020 https://bit.ly/3KwYDnR; Waldman, Ari Ezra, 'Privacy, Practice, and Performance', California Law Review, Vol. 110 2021, https://ssrn.com/abstract=3784667; Jamie Luguri and Lior Jacob Strahilevitz, 'Shining a Light on Dark Patterns', Journal of Legal Analysis, Volume 13, Issue 1, 2021, Pages 43–109 https://bit.ly/3FL9pn8

[79] Future of Privacy Forum Comments, California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments – Part One, 8 November 2021, https://bit.ly/3KlOKcQ; Giovanni Sartor, Francesca Lagioia, Federico Galli, 'Regulating targeted and behavioural advertising in digital services: how to ensure users' informed consent', European Parliament, JURI, July 2021, 4.3.2 https://bit.ly/3FI4iUJ; Maureen Mahoney, 'California Consumer Privacy Act: Are Consumers' Digital Rights Protected?', Consumer Reports & Digital Lab, 1 October, 2020 https://bit.ly/3s8pcsn; 韩旭至, '个人信息保护中告知同意的困境与出路', 经贸法律评论, 2021 年第 1 期 http://law.uibe.edu.cn/docs//2021-03/4068d9f7a91a4892811817d59e56459a.pdf

[80] 'Out of Control: How consumers are exploited by the online advertising industry', Norwegian Consumer Council, 14 January 2020 https://bit.ly/3BpDqYO

[81] Privacy Coalition Comments, California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments – Part One, 8 November 2021, https://bit.ly/3KlOKcQ

[82] Edwards, Lilian and Veale, Michael, Enslaving the Algorithm: From a 'Right to an Explanation' to a 'Right to Better Decisions'? (2018). IEEE Security & Privacy (2018) 16(3), pp. 46-54, https://ssrn.com/abstract=3052831; Julie Cohen, 'How (Not) to Write a Privacy Law', Knight Institute and Law and Political Economy Project, March 2021 https://knightcolumbia.org/content/how-not-to-write-a-privacy-law; Viljoen, Salome, Democratic Data: A Relational Theory For Data Governance (Yale Law Journal, Forthcoming, https://ssrn.com/abstract=3727562

[83] Julie Cohen, 'How (Not) to Write a Privacy Law', Knight Institute and Law and Political Economy Project, March 2021 https://bit.ly/3tSufOO

in other simpler contexts, this assumption has become an intractable knot at the centre of current efforts to use data protection law to reform behavioural advertising.

However flawed notice and consent / choice might be as a basis for legitimising data sharing for behavioural advertising purposes, the model is deeply embedded in consumer law generally as much as data protection law across all four jurisdictions. Not surprisingly, the primary effort so far has therefore been directed at mitigating consumer incapacity rather than replacing notice and consent / choice.[84] The regulation of 'dark patterns', the manipulation of online consumers through deceptive notice and consent interfaces described above, is a leading example of this drive to mitigate consumer incapacity. While the concept of dark patterns was first recognised as a specific data protection law issue in the United States,[85] regulators in the UK, EU and China are equally focused on these kinds of notice and consent abuses regardless of the label.[86] Serious abuses in China, for example, include text that is deliberately difficult for users to read (e.g. overly small or dense, light in colour, fuzzy or only provide in traditional rather than simplified Chinese characters) or difficult to access (e.g. only reached after numerous clicks), or information notices that do not include data subject rights or impose unreasonable conditions and burdensome procedures for the exercises of those rights.[87]

Left unregulated, online notice and consent / choice interfaces have provided numerous ways for online publishers and advertisers to game consumer incapacities to favour opting into behavioural advertising and disfavour opting out. In these circumstances, the mass effect of non-deliberative, individual decision-making has favoured the continuing viability of behavioural advertising systems. Yet, recent regulatory consultations in California regarding legal prohibitions on the use of dark patterns indicate the difficulties of eliminating deceptive notice and consent interfaces. These include -

[84] Finck, Michèle, The Limits of the GDPR in the Personalisation Context (May 1, 2020). Forthcoming in: U. Kohl, J. Eisler (eds), Data-Driven Personalisation in Markets, Politics and Law, Cambridge: Cambridge University Press, 2021, Max Planck Institute for Innovation & Competition Research Paper No. 21-11, Available at SSRN: https://ssrn.com/abstract=3830304

[85] FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions, October 28, 2021 https://bit.ly/353ACVs; Attorney General Becerra Announces Approval of Additional Regulations That Empower Data Privacy Under the California Consumer Privacy Act, 15 March 2021 https://bit.ly/3GQB8mQ; Adi Robertson, 'Google sued by DC and three states for 'deceptive' Android location tracking', 24 January 2022, The Verge https://bit.ly/3rW82hx; Colorado Attorney General, Pre-Rulemaking Considerations for the Colorado Privacy Act, 12 April 2022 https://bit.ly/3vDWG2w

[86] James Vincent, 'France fines Google and Facebook for pushing tracking cookies on users with dark patterns' The Verge, 7 January 2022 https://www.theverge.com/2022/1/7/22871719/france-fines-google-facebook-cookies-tracking-dark-patterns-eprivacy; EDPB, Guidelines 3/2022 on dark patterns in social media platform interfaces: How to recognise and avoid them Version 1.0, 14 March 2022 https://bit.ly/3xNm3lc; Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations." (App 违法违规收集使用个人信息行为认定方法), http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm; "Notice of the Ministry of Industry and Information Technology on launching special rectification work for APP infringing on the rights and interests of users." (工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知) http://www.gov.cn/fuwu/2019-11/07/content_5449660.htm

[87] See Annex Three

- When does information provided to inform decision making become excessive and impair autonomy, decision-making and choice?

- To what extent should opt out mechanisms provide single choices for all aspects of processing for advertising purposes to enable granular rather than blanket choices?

- Should clickable opt out buttons be provided on every page of an online consumer service or is it sufficient to provide those buttons on the first page?

Efforts to counter the use of dark patterns have tended towards standardised, streamlined notice and consent features in online interfaces (sometimes called 'bright patterns').[88] The problem here is that bright patterns can also be criticised for neither expecting nor enabling informed, deliberative decision making. If the objective is to dismantle behavioural advertising completely, it is certainly logical to push for mandatory prominent, clickable 'reject tracking' options, which consumers are likely to choose regardless of lack of their knowledge of the specific consequences. As noted, the incapacity of consumers tends to promote a form of automated decision making through unreasoned mass effects, which can be gamed for wider societal objectives as much as for more narrow commercial ones. Whatever the merits of those societal goals, including elimination of pervasive commercial surveillance, the method raises questions about both commending informed personal choice and relying on instinctive, non-deliberative consumer choices to achieve a policy goal – the demolishing the Real Time Bidding system through the mass effect of one click rejections of tracking. At some point, this strategy may come back to bite its proponents.

This discussion should not give the impression that the eventual consensus in these four jurisdictions on the contours of legitimate behavioural advertising is entirely in the hands of their data protection legislators and regulators or, less significantly for China, their courts through privacy activist litigation. Major online platform and operating system companies and, to a lesser extent, advertising tech companies, have many advantages in the current struggle to re-set the rules for legitimate behavioural advertising.[89] Although under serious regulatory pressure,[90] IAB TechLab's 'Consent and Transparency Framework' (currently TCF 2.0), for example, has provided a standard in Europe for behavioural advertising notice and consent mechanisms, including the role of Consent Management Providers (CMPs), who implement the framework on individual websites.[91] The creation of standards

[88] Paul Graßl, Hanna Schraffenberger, Frederik Zuiderveen Borgesius & Moniek Buijzen, 'Dark and Bright Patterns in Cookie Consent Requests' Journal of Digital Social Research, Vol. 3: No. 1: 2021
[89] Joris van Hoboken and R.O Fathaigh, 'Smartphone platforms as privacy regulators', *Computer Law & Security Review,* Volume 41, July 2021
[90] APD/GBA (Belgium), Decision on the merits 21/2022, Concerning: Complaint relating to Transparency & Consent Framework, 2 February 2022 DOS-2019-01377 https://bit.ly/3k7RMFp; IAB Europe, Belgian DPA ("APD") Decision on IAB Europe and the TCF: IAB Europe Submits Action Plan, A Key Milestone in the Process, 1 April 2022 https://bit.ly/3vcndVD
[91] Célestin Matte, Cristiana Santos, Nataliia Bielova. 'Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?', APF 2020 - Annual Privacy Forum, Oct 2020, Lisbon, Portugal. pp.1-24. https://hal.inria.fr/hal-02566891/document

and mechanisms by major tech companies, as well as advertising industry associations, have been highly effective in pre-emptively setting de facto implementation standards for data protection law in relation to behavioural advertising.[92] Data protection regulators, moreover, choose their targets selectively. Major tech companies are usually better resourced and often likely to appeal adverse regulatory decisions in potentially drawn out regulatory and judicial proceedings.

8. Running to stay in the same place?

It is still early days to make conclusive comparisons regarding consumer data protection law in the U.S. and China as compared to the UK and the EU. In the former, the meaning and application of rights and duties introduced by data protection legislation enacted in the past year are still being worked out. Nonetheless, the California Privacy Rights Act Proposed Rulemaking[93] and China's Special Rectification Scheme for Mobile Apps[94] give some useful indications of how behavioural advertising issues are likely to be addressed by regulators in those jurisdictions. Specific outcomes on particular issues will no doubt diverge, reflecting differences in legal texts, contexts and policy preferences, but parallel conclusions are also likely, given the similarities in how behavioural advertising systems operate and key similarities in their data protection regimes as they apply in online consumer contexts. The problem of how to empower increasingly incapacitated consumers within the notice and consent / choice rules of their consumer data protection regimes is undoubtedly a shared one. All four jurisdictions are therefore confronting similar legal and technical questions regarding the future role of consumer autonomy and choice mechanisms in the face of potential deceptive manipulation as compared to protective regulation that effectively overrides and channels consumer decision making. This is also a shared point of decision regarding the legitimacy of alternatives to the now discredited third party tracking model, which nonetheless rely on first party data derived from the personalisation of consumer services to enable new forms of targeted advertising. Given the importance of advertising in making digital services more affordable, even in Europe, contentious compromises can be expected.

The following sections illustrate some of these key issues. Looked at as a whole, they illustrate that individual consumer autonomy in the form of genuinely well informed, deliberative choice is not a realistic, long-term solution to the problem of determining the legitimate nature and scope of behavioural advertising. In these circumstances, current efforts to mitigate the weaknesses of notice and consent in complex online environments give the appearance of running to stay in the same place. Each legal and technical issue seemingly resolved through legislative or regulatory intervention (e.g. the EU ePrivacy Directive cookie consent requirement) has sparked commercial innovations that

[92] Maximilian Hils, Daniel W Woods, and Rainer Böhme. Measuring the Emergence of Consent Management on the Web, IMC '20: Proceedings of the ACM Internet Measurement Conference October 2020 https://doi.org/10.1145/3419394.3423647
[93] California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments, https://cppa.ca.gov/regulations/
[94] See Annex three

seek new ways to exploit the weaknesses of consumer data protection's commitment to informed consent / choice as a primary mechanism of control. Constant regulatory repair is, consequently, an ongoing necessity, including current efforts to limit deceptive 'dark pattern' interfaces. In the longer term, as networked, personalised devices, services and environments continue to develop, alternative ways of addressing the potential harms of advanced data analytics are more likely to provide more effective solutions. These alternatives are discussed below.

Definitional boundaries

While notice and consent / choice rules are the core of consumer data protection law, they also sit within a larger architecture that determines their scope and how they operate. In determining what matters fall within the scope of consumer opt in or opt out choices, including the range of information consumers must receive at the point of decision when given the option of sharing their data with advertisers, definitions have a particularly important role. Definitional distinctions between personal, anonymous and pseudonymous data are, moreover, central to efforts to rehabilitate or dismantle behavioural advertising. In principle, data that is indisputably not 'personal data' or 'personal information' is outside the scope of data protection law.[95] Yet, the essence of targeted behavioural advertising is personalisation and complete anonymisation of data would defeat its purposes. Anonymisation and possibly pseudonymisation, however, holds out the promise of enabling the sharing of unidentifiable data between the unnumerable parties operating in behavioural advertising systems, while still preserving personalisation at the point of advertising targeting and attribution, provided these processes are kept separate. In short, consented personal data can potentially be anonymised or de-identified for sharing purposes or used for other innovations in advertising methods by working the definitional boundaries of data protection law.[96] Innovations of this kind are also likely to feature in forms of artificial intelligence based 'contextual' advertising that ostensibly meet the demands of regulators and privacy organisations, while also continuing to enable indirect targeted advertising.[97]

Yet, using anonymisation to sustain re-constructed forms of behavioural advertising requires legal as well as technical expertise. Much depends on the extent to which definitions of personal data or personal are absolute or relative.[98] In other words, in whose hands or at one point

[95] GDPR Article 4(1), CCPA 1798.140(m) and (v), PIPL Article 4.
[96] See, for example, planned innovations for intelligent contextual' advertising - Bruce Biegal and Charles Ping, 'The Outlook for Contextual Solutions in Data Driven Advertising & Marketing', Winterberry Group, October 2021 https://bit.ly/3fxKvwq
[97] Kabir Ahuja, Thomas Bauer, Caroline Meder, and Oliver Gediehn, 'As the cookie crumbles, three strategies for advertisers to thrive' McKinsey. 6 April, 2022 https://mck.co/3Lba98h
[98] ICO draft guidance: Anonymisation, pseudonymisation and privacy enhancing technologies guidance (chapters two and three) https://bit.ly/3sb729D; Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, (CJEU) 19 October 2016; Michele Finck and Frank Pallas, 'They who must not be identified — Distinguishing personal from non-personal data under the GDPR', *International Data Privacy Law,* 2020, Vol. 10, No. 1.; Electronic Frontier Foundation (EFF) and ACLU California Action Comments, California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments – Part One, 8 November 2021, https://bit.ly/3KlOKcQ

does personal data become sufficiently anonymous that data protection law no longer applies for at least certain processing activities? An absolute approach is likely to be over inclusive and capture low risk, unintentional processing, while the flexibility of a relative approach may be under inclusive and invite exploitation for harmful purposes. The Belgian data protection authority's decision regarding IAB Europe and its Transparency and Consent Framework as well as the Austrian DPA's decision regarding Google Analytics indicate that European regulators are shifting towards a more absolutist view of personal data.[99] Definitions of 'personal information' or 'personal data' in the United States and China are sufficiently similar to the GDPR in key concepts that same questions arise. So far, they are not as contentious. It is, however, likely that there will be a spectrum of regulatory views on whether anonymised data is more relative or absolute.

Google, through its Privacy Sandbox for the Chrome browser, is currently providing the leading example of efforts to develop an anonymous data interface that will enable targeted advertising to continue without the need for consent to direct sharing of personal data. Google's 2021 attempt to create an anonymous data interface in the form of its federated learning solution (Federated Learning of Flocks - FLoC) failed in the face of determined opposition from critics who argued that its apparent anonymisation of consumer preferences could be reverse engineered by third party data brokers and advertisers.[100] Google recently withdrew the FLoC proposal and advanced a new concept - 'Topics' to provide an anonymous data interface for advertisers, which is intended to will enable a modified form of behavioural advertising with less risk of reverse engineering than the FLoC concept.[101]

In the mobile app sphere, following its restrictions on app based tracking noted above, Apple created a new interface (SKAdNetwork) for advertisers that similarly shares de-identified data with advertisers to enable a degree of effective targeting of Apple device users.[102] Google has responded with announcements of work on data protection compliant solutions for data sharing in Android mobile operating system contexts.[103] Privacy compliance as a business model is nonetheless costly. Solutions using de-dentification, for example, require technical skills and resources that are typically the preserve of major tech businesses (e.g. data clean rooms - Google Ads Data Hub) or at least the agreement of major platforms and operating systems to facilitate their operation.[104]

---

[99] (Belgium) Autorité de protection des données (APD), Complaint relating to Transparency & Consent Framework, Case number: DOS-2019-01377, 2 February 2022 https://bit.ly/3JuvMiJ; Österreichische Datenschutzbehörde, NOYB European Centre for Digital Rights, D155.027, 2021-0.586.257, 13 January 2022 https://bit.ly/3JyFYXA

[100] Eric Rescorla, 'Privacy analysis of FLoC', Mozilla 10 June, 2021 https://blog.mozilla.org/en/mozilla/privacy-analysis-of-floc/; Eric Rescorla and Martin Thomson, 'Technical Comments on FLoC Privacy', Mozilla 10 June, 2021 https://mozilla.github.io/ppa-docs/floc_report.pdf

[101] Vinay Goel, Get to know the new Topics API for Privacy Sandbox, Google, 25 January 2022 https://bit.ly/3BwkoAo; The Topics API, GitHub https://github.com/patcg-individual-drafts/topics

[102] John Koetsier, 'Apple's Ad Network Is The Biggest Beneficiary Of Apple's New Marketing Rules: Report', Forbes, 19 October 2021 https://bit.ly/3uXjkUB

[103] Anthony Chavez, 'Introducing the Privacy Sandbox on Android', Google, 16 February 2022 https://bit.ly/3HYRxXL

[104] Future of Privacy Forum Comments, California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments – Part One, 8 November 2021, https://bit.ly/3KlOKcQ

Definitions for ‘personal data’ and ‘personal information’ as well as complementary concepts, such as anonymisation and de-identification in relation to data sharing, are consequently key elements in the design of next generation behavioural advertising. Other data protection definitions operate in inverse ways, creating areas of high risk for data controllers and processors, which also need to be legally and technically managed. The GDPR,[105] CCPA[106] and PIPL definitions of special category or sensitive data are, for example, broadly comparable and carry additional duties for data controllers. The CCPA, for example, which contains more detailed stipulations than the broad-brush GDPR and PIPL, introduces other definitions and terms that are already the subject of disagreement in its rule making consultations, such as ‘cross-context behavioural advertising’, ‘target’ and ‘dark pattern’.[107]

Conditions, limitations and mechanisms for consent

Beyond the meaning of definitions and terms, which determine when and how rules apply, the core issue for data protection based regulation of behavioural advertising is how to enable more meaningful consumer opt ins and opt outs. Meaningful notice and consent or choice in this context has two aspects: what conditions or limitations should be placed on consumer rights to opt in or opt out; and, what mechanisms ought to be used to ensure meaningful consumer decision making when opting in or opting out. In both aspects, solutions need to avoid imposing excessive demands on consumers or burdens on service providers in the effort to support informed and freely decided consumer choices. Additionally, solutions for behavioural advertising must also avoid placing unintended restrictions on first party marketing of services to customers or on other first party personalised services, such as recommender systems, which also observe and infer individual behaviour, interests, preferences and now, potentially, individual emotions and intentions. Consequently, the focus has been on informed consent or choice regarding the sharing of first party data with third parties through forms of cross web and cross app tracking, which is in principle distinguishable from first party personalisation. On the other hand, protected categories, such as sensitive personal data and children’s personal data, are increasingly significant for the regulation of first party personalised services, indicating the regulatory direction of travel.

Across all four jurisdictions, the legislative and regulatory focus has increasingly shifted towards the mechanics of opting in or opting out of personal data sharing with third parties for advertising purposes. This shift has come about for obvious reasons. The early adoption and continuing insistence on the primary role of informed consent or choice in consumer data protection law brought the embedded problems of consumer law into data protection law. While behavioural advertising may have its origins in the observant shopkeeper, it was the invention of third party cookies in 1996 that created the technical basis for its explosive development as a key part of the internet era. As noted

[105] GDPR, Article 9
[106] CCPA 1798.121. Note that the California Genetic Information Privacy Act 2021 adds a consent (opt in) requirement for direct-to-consumer genetic testing companies https://bit.ly/3FyuZuJ
[107] CCPA 1798.140(k); Wilson Sonsini Comments, California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments – Part One, 8 November 2021, https://bit.ly/3KlOKcQ

above, the subsequent development of mobile apps and their associated data sharing technologies, such as SDKs, significantly extended the reach of nascent behavioural advertising systems, especially in China. To ensure a constant flow of personal data into these systems, many online service providers adopted complex, opaque and confusing privacy notices.[108] The consequent bewilderment of online consumers meant that consent to share, whether as implicit consent in the U.S. or as explicit consent in Europe and China, was often a parody of informed decision making.

This well known history led to a tightening series of judicial, regulatory and industry interventions that are now re-shaping online notice and consent / choice interfaces across the four jurisdictions. In simple terms, this has meant an intense focus on one click solutions for consumers to avoid unwanted data sharing for advertising purposes. In Europe, the combination of GDPR and ePrivacy Directive requirements for express consent for specific requests to data subjects to share personal data created, first, the conditions for an industry strategy of presenting online users with prominent 'accept all' one click options[109] and, second, a regulatory response requiring equally prominent 'reject all' one click options.[110] This contingent regulatory response is based on mutuality: service providers must make it as easy for online consumers to refuse or withdraw consent as they make it easy to consent. European data protection authorities have, however, had much less success in finding ways to enforce the GDPR Article 21 right of online consumers to object to direct marketing by automated means,[111] despite considerable efforts to regulate website and mobile app interface design.[112]

Developments in the United States underscore the limitations of current European reliance on a contingent one click solution. All four of the U.S. state level consumer privacy acts create rights to opt out of the sale of personal data to third parties for advertising purposes, which in the case of California and Colorado are also directly linked to one click online opt outs. These legislated opt out rights vary in their breadth and conditions, but nonetheless mark a decisive legislative intervention into the problem of consumer confusion and incapacity when negotiating online notice and consent / choice interfaces. They also signal a closing divide between European and American consumer data protection, offering a simple opt out at the time of initial data collection that will operate similarly to

---

[108] McDonald, A.M., Reeder, R.W., Kelley, P.G., Cranor, L.F, 'A Comparative Study of Online Privacy Policies and Formats', (In Goldberg, I., Atallah, M.J. (eds) Privacy Enhancing Technologies PETS 2009. Lecture Notes in Computer Science, vol 5672); Joel R. Reidenberg, et al, 'Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding', Berkeley Technology Law Journal, Vol. 30, No. 1 (Spring 2015), 39

[109] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 'Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence', 2020 https://arxiv.org/pdf/2001.02479.pdf

[110] CNIL, Cookies: the CNIL fines GOOGLE a total of 150 million euros and Facebook 60 million euros for non-compliance with French legislation, 6 January 2022 https://bit.ly/3JRn7YR

[111] Natasha Lomas, 'Europe needs to back browser-level controls to fix cookie consent nightmares, says privacy group', 14 June 2021 https://tcrn.ch/3LBqIdR

[112] Case C-673/17, *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V,* 1 October 2019, CJEU ; EDPB - Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019 https://bit.ly/3r43GTV; EDPB - Guidelines 8/2020 on the targeting of social media users, Version 2.0, 13 April 2021, 54-55 https://bit.ly/3neiUEW; ICO Guidance on the use of cookies and similar technologies, https://bit.ly/352W8JR; CNIL Cookie guidelines - Délibération n° 2020-091 / Délibération n° 2020-092 https://bit.ly/3rqw1Ed; Mariano Delli Santi, 'Eprivacy Regulation and Privacy Automation', Open Rights Group, 1 June, 2021 https://bit.ly/3tOMftx

parallel European refusal to consent options. The comparative strength of these U.S. opt outs is that they apply regardless of how the relevant personal data is collected, unlike solutions that are based on a process mutuality of consent and refusal options. That said, Google's recently announced roll out of a 'reject all' option for users of Google search and YouTube in Europe is a direct response to the CNIL's insistence that refusal of consent should be as easy as giving consent.[113]

The application breadth of U.S. state level opt outs from personal data sharing have also created a wider range of implementation issues than as yet encountered by European regulators. In Europe, where ease of refusal or withdrawal of consent typically occurs in the context of a user interface intended to gain legitimate consent of identifiable users, the service provider is already in possession of sufficient information about the user necessary to honour a refusal to consent. A broader opt out right will, however, arise in circumstances where user identity is potentially uncertain. In California, the question of how to resolve that uncertainty has provoked different views on what information should be provided to ensure informed, authenticated opt outs without creating barriers to user choice. In the California Privacy Protection Agency's recent rule making consultation, for example, the modalities of opting in and opting out of personal data sharing for advertising purposes attracted considerable comment –

- Is initial consent to first party processing for advertising purposes limited to the service the consumer intentionally contacts or does it include services operated by the same provider?

- How much information is necessary for informed opt outs, given the potential cost burdens on service providers required to provide such information?

- Should consumers be required to authenticate their identity before data controllers facilitate an opt out?

- How much information should controllers be allowed to provide to consumers wishing to opt out without creating barriers to opt out?

- In what circumstances is it legitimate to deny access to a free service for consumers who opt out of data sharing for advertising purposes (tracking walls)?

In California and Colorado, in creating rights to opt out by using a one click online option, the state legislatures also opened the way for regulatory approval of automated, universal opt out signals

[113] Sammit Adhya, 'New cookie choices in Europe', Google, 21 April 2022 https://bit.ly/3L7H0Lv; See also, Belgian DPA ("APD") Decision on IAB Europe and the TCF: IAB Europe Submits Action Plan, A Key Milestone in the Process, 1 April 2022 https://bit.ly/3rLu5XJ; Russell Ketchum, Prepare for the future with Google Analytics 4, Google, 16 March 2022 https://bit.ly/3FdTChI

('global privacy controls' or GPCs).[114] GPCs are intended to provide a 'privacy enhancing technology' (PET) solution to the problems of interface complexity and opacity as well as consumer decision making fatigue, working across websites through browser or mobile app generated signals. Yet, as the California rule making consultation has shown, even for this relatively narrow issue, there are major interpretational and technical obstacles -

- Must consumers authenticate their identity when using an automated universal opt out signal?
- Must a data controller send a confirmation signal to the consumer in response to a universal opt out signal?
- What form of universal signal must be generated to be valid?
- How many different forms of valid universal signal must a data controller honour?
- What different devices will be able to generate and send such signals?
- How will cross device recognition be enabled without divulging consumer identities?
- How will signals be passed through machine-to-machine communication as advertising supported smart services, devices and environments increase?
- Should opt out signals override agreement to privacy policies through user registration?

The Colorado Attorney General has begun preparations for rule making under the authority of the Colorado Privacy Act under legislated provisions the display similar concerns.[115] These provisions, for example, require that the rules must not adopt a mechanism that is a default setting, but rather clearly represents the consumer's affirmative, freely given, and unambiguous choice to opt out of the processing of personal data.[116] As this requirement demonstrates, autonomous decision making is a double edged concept that can be expected to set limits on the development of easy access, one click opt outs that have universal effect to block data sharing for advertising purposes.[117] In its recent decision regarding IAB Europe, the Belgian data protection authority indicated that, in relation to

[114] Russell Brandom, 'Global Privacy Control Wants to Succeed where Do Not Track Failed' The Verge, 28 January, 2021 https://bit.ly/3fFXc8H; Global Privacy Control - Take control of your privacy https://globalprivacycontrol.org; NOYB - New browser signal could make cookie banners obsolete https://bit.ly/33EzI13
[115] Colorado Attorney General Office, Pre-Rulemaking Considerations for the Colorado Privacy Act https://bit.ly/3k4PuqA
[116] Colorado Privacy Act, § 6-1-1313 Rules - Opt out mechanism
[117] On the challenges of making PETs effective, see, Nitin Agrawal, Reuben Binns, Max Van Kleek, Kim Laine, and Nigel Shadbolt, 'Exploring design and governance challenges in the development of privacy-preserving computation', Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, 1 https://arxiv.org/pdf/2101.08048.pdf

consent to the use of browser cookies for advertising purposes, there should be a 'unified user interface' across all online publishers.[118] Early experience in the United States indicates that the dual goal of informed, meaningful consumer choice that is facilitated through easily recognised, understood and operated interfaces will need to confront the question of how the tensions between those goals can be addressed.

The experience in China, where opt outs requirements are now even broader than those mandated in U.S. consumer privacy laws, is equally illustrative of the challenges in moves towards simplified online opt out mechanisms. Article 24 of the Personal Information Protection Law (PIPL) of 2021 created an obligation for entities conducting information push delivery or commercial sales to individuals through automated decision-making methods to provide an option to not target an individual's characteristics or to provide the individual with a convenient method to refuse. Building on the PIPL and other information sector legislation, the regulatory Provisions on the Management of Algorithmic Recommendation in Internet Information Services, which came into effect on 1 March 2022, have propelled the requirement for user opt out mechanisms further forward.[119] Article 17 of these regulations require that algorithmic recommendation service providers either to provide users with an option to not target their individual characteristics or to provide users with a convenient option to switch off algorithmic recommendation services. Behavioural advertising is thus only one element in this drive towards mandatory one click opt outs in China .

While not directly attributed to these new rules, major online service providers in China have begun to provide one click opt outs from personalised recommendations in mobile app user interfaces.[120] This major leap in the empowerment of consumers to reject automated personalisation, extending well beyond third party targeting for advertising purposes to all recommender systems. Recognising the potential impact on first party services in which recommender systems are integral to basic functionality, many services providers are creating two single click opt out options – one for behavioural advertising and one for content recommendation.[121]

9. Harms based solutions

Legislative, judicial and regulatory pressures, in combination with operational changes introduced by major tech platform and system providers, are now breaking down Real Time Bidding systems. The push to introduce one click consent refusal or opt out solutions to cross web and cross app tracking has played a major part in this growing success, empowering consumers to act on their dislike of RTB's crude and ubiquitous tracking. Despite tenacious resistance, RTB systems were always highly vulnerable to informed consumer consent or choice. They developed as systems of surveillance

[118] (Belgium) Autorité de protection des données (APD), Complaint relating to Transparency & Consent Framework, Case number: DOS-2019-01377, 2 February 2022 https://bit.ly/3JuvMiJ
[119] See Annex Two.
[120] 各大 APP 允许用户一键关闭"个性化推荐"后，还会有"大数据杀熟"吗？ https://bit.ly/3s96Bw7
[121] 各大 APP 允许用户一键关闭"个性化推荐"后，还会有"大数据杀熟"吗？ https://bit.ly/3s96Bw7

hidden from online consumers and largely without regard to non-existent or weakly enforced data protection rules. Once simple to operate notice and consent / choice mechanisms are in place, their impact on RTB systems has been devastating. In the next behavioural advertising era, the mechanisms of data extraction, profiling and targeting will be better designed to navigate notice and consent / choice requirements and better adapted to exploit increasing consumer incapacities in complex digital environments.[122] In this dawning era, legislative and regulatory management of online notice and consent / choice interfaces is unlikely to be a viable long-term strategy.

Across the four jurisdictions discussed in this study, there is undoubtedly a broad awareness of this problem as well as an evident emergence of an alternative harms based approach to behavioural advertising. These include variety of legislative, judicial and regulatory interventions, described below, that limit harmful practices and in different ways restrict the possibilities for exploiting consent and choice. These include use of principles of fairness and reasonableness, the creation of protective regimes for vulnerable groups, especially children, and the introduction of risk based regulation for artificial intelligence. Undoubtedly, given consumer data protection law's structural commitment to notice and consent / choice frameworks, these harms based solutions will surround and overlay with rather than replace those frameworks.

Consumer data protection is certainly more than notice and consent / choice requirements, although in the United States federal law has struggled to develop beyond that core element.[123] Principles of fairness and reasonableness as well as purpose limitation and data minimisation are present to different degrees in data protection laws across the four jurisdictions under discussion.[124] In combination, these principles have been deployed in the UK and EU to define and structure notice and consent to strengthen the controller's procedural and substantive responsibilities.[125] Whether regulators and courts in the United States and China will use fairness, reasonableness, purpose limitation and data minimisation in similar ways is not yet clear. The concept of a 'reasonable expectation of privacy" is already well developed in California privacy tort law and can be expected to

[122] CNIL, 'Alternatives to third-party cookies: what consequences regarding consent?' 23 November 2021 https://bit.ly/3vFz6DO
[123] Commissioner Rebecca Kelly Slaughter, 'Wait But Why? Rethinking Assumptions About Surveillance Advertising', IAPP Privacy Security Risk Keynote 22 October, 2021 https://bit.ly/3BP3du1
[124] Fairness, for example, is found in GDPR Article 5(1)(a) and PIPL Articles 24 and 58, while the concept of 'reasonable' is used in the CCPA in relation to specific obligations or conditions: e.g., CCPA 1798.185 (10) authority to issue regulation that align business purposes with consumer expectations
[125] See, for example, Case C-673/17, *Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V,* 1 October 2019, CJEU; EDPB - Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, Para 12 and footnote 8 https://bit.ly/3r43GTV; EDPB - Guidelines 8/2020 on the targeting of social media users, Version 2.0, 13 April 2021, Para 10 and 86 https://bit.ly/3neiUEW; Article 29 Working Party, Opinion 03/2013 on purpose limitation, p. 46, 2 April 2013 https://bit.ly/3tTQjJh: EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, Section 3.1.3 Granularity https://bit.ly/2TqCsXg; Isabel Hahn, 'Purpose Limitation in the Time of Data Power: Is There a Way Forward?', European Data Protection Law Review, Volume 7 (2021), Issue 1; Asia Biega & Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems. Technology and Regulation, 2021, 44–61

figure in the interpretation of the CCPA.[126] In China, there is a strong academic awareness of how fairness and reasonableness principles might affect the interpretation of data protection laws, which indicates regulatory awareness as well.[127]

Fairness, trust, reasonableness and other general principles have considerable potential to change the nature of consumer data protection through regulatory and judicial intervention. If pursued expansively, principles could be used to impose major substantive prohibitions on demonstrably harmful as well as high risk consumer choices within online notice and consent / choice mechanisms that would restrict new adaptations in behavioural advertising.[128] This would no doubt make the continual repair of notice and consent / choice frameworks less arduous.[129] Although it is important not to overlook the double edged character of the reasonable expectation principle. The new Utah Consumer Privacy Act, for example, creates an exception to its restrictions on sharing personal data with third parties if the purpose of the sharing is consistent with a consumer's reasonable expectations.

In any event, a principled based interpretational strategy harbours a more significant problem. Notice and consent / choice mechanisms are intended to support individual autonomy or informational self-determination in consumer decision making. Regulatory or judicial declarations regarding fairness or the reasonable expectations of consumers, consequently, risk being challenged that they are value based conclusions that over-ride consumer choice without sufficient evidential basis. This is, in effect, a move beyond direct empowerment of individual decision-making to a more paternalist safeguarding of a modified sphere of individual autonomy with high risks of perceived arbitrariness.[130]

Undoubtedly, key privacy concepts, such as 'contextual integrity', do focus on the importance of societal norms regarding appropriate uses of personal data in different contexts (e.g. personalisation of a digital assistant as compared to the use of the same data for behavioural advertising).[131] The difficulties lie in identifying and then applying those norms in convincingly objective ways. Paternalism is of course an unavoidable and even necessary feature of governance, but the manner in which it is

---

[126] *Shulman v. Group W Productions, Inc.,* 955 P.2d 469 (1998), Supreme Court of California https://bit.ly/3AhhD53

[127] 张新宝：个人信息处理的五项基本原则', 中国法律评论, 2021 年第 5 期（总第 41 期）https://wemp.app/posts/750fe40b-0b08-4778-b298-aca27c1e093d; 王利明, '论美国隐私权法中的合理期待理论, 中国民商法律网, 2020 年 12 月 12 日 https://www.civillaw.com.cn/bo/t/?id=37410; 张新宝, '个人信息收集：告知同意原则适用的限制', 民事法学, 10 December 2019 : https://www.civillaw.com.cn/zt/t/?id=36378

[128] Coalition Letter - Ban Surveillance Advertising, 23 June 2021 https://bit.ly/3KtHQSz; Norwegian Consumer Council, Time to Ban Surveillance-Based Advertising, 22 June 2021 https://bit.ly/3ImZMg1

[129] Note that even strongly worded initiatives aimed at banning all pervasive tracking of consumers make exceptions for tracking necessary for service provision and billing, indicating the difficulties of applying simple prohibitive solutions to personalisation in first party consumer relationships: See, 'Justification' in Digital Services Act - LIBE Opinion, Rapporteur: Patrick Breyer, 11.7.2021 https://www.europarl.europa.eu/doceo/document/LIBE-PA-692898_EN.pdf

[130] Pranvera Këllezi, 'Consumer Choice and Consent in Data Protection' Antitrust Chronicle, January 2021 https://bit.ly/3I9D6Qu

[131] Oskar Josef Gstrein and Anne Beaulieu, 'How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches', Philosophy & Technology (2022) https://bit.ly/3h3YUkU

exercised has major implications for its legitimacy. Although similar in aims to unfair contract terms laws,[132] principles based regulatory and judicial restrictions on the scope of individual consent or choice can be open-ended and non-democratically accountable.

Plainly, liberal democratic objections of this kind are not internally relevant to China's policy, legal and regulatory decision-making processes. Setting aside the degree to which broader Chinese societal values may support paternalism over autonomy, authoritative paternalist intervention is a mainstay of the Party-state's governance. Nonetheless, the effects of arbitrary and unpredictable interventions on the development of the digital economy are a concern within China and can be expected to influence how the fairness and reasonableness principles of the PIPL are implemented.

Data protection law has provided a different avenue for harms based interventions that are grounded in explicit rules concerning the protection of vulnerable groups, including in particular children.[133] In recent years, the protection of children from online exploitation has become a key policy issue that has brought significant changes to content responsibility and liability rules.[134] In relation to cross web and cross app tracking for advertising purposes, protections for children have tended to emphasise informed parental choice / consent, although increasingly restrictive measures that override consent or choice are being introduced. In addition to basic data protection rules regarding children, existing and proposed measures include -

- UK ICO Children's Code / Age Appropriate Design Code, effective 2 September 2021 https://bit.ly/3saBUXi
- EU Digital Services Act 2022 (ban on targeted advertising aimed at children) https://bit.ly/3sc9L1V
- California State Legislature, AB-2273 California Age-Appropriate Design Code Act bill https://bit.ly/3vZgBsJ
- U.S. Congress, S.3663 - Kids Online Safety Act Bill https://bit.ly/3vFhNCD
- China, Provisions on the Cyber Protection of Children's Personal Information, Effective 2019 https://bit.ly/3LYDt2B (See Annex Two)
- China, Revised Regulation on the Online Protection of Minors, March 2022 https://bit.ly/3LKrXrm

Outside the data protection law sphere, but overlapping with many of its concerns, risk regulation of artificial intelligence offers the possibility of a harms based approach to behavioural advertising.[135]

[132] Unfair Contract Terms Directive 93/13, Art. 3(1)
[133] Article 29 Data Protection Working Party Guidelines on Automated Individual decision-making and Profiling for the purposes of Regulation 2016/679, Chapter V https://bit.ly/3LHE5ZX
[134] See, for example, the UK Online Safety Bill https://bills.parliament.uk/bills/3137/publications; John Woodhouse 'Regulating Online Harms', Parliamentary Research Briefing, 15 March 2022 https://bit.ly/3EWc8vf
[135] Daniel Zhang, et al, 'The AI Index 2022 Annual Report', AI Index Steering Committee, Stanford Institute for Human-Centered AI, Stanford University, March 2022 https://stanford.io/3LHMf4L

The data protection laws discussed in this report all contain specific provisions regarding automated decision-making, although the UK government has proposed modifying these provisions in the UK GDPR.[136] However, these provisions not only depend on consumer notice and choice / choice, but also are typically conditioned on whether they cause legal or other significant effects, which excludes most automated decision-making in behavioural advertising.[137] Interestingly, the CCPA does not restrict its automated decision-making provisions in this way, which is a major point of contention in CCPA rule making consultation.[138]

New legislative or regulatory initiatives for risk regulation of artificial intelligence would overcome the limitations of this notice and consent, rights based approach[139] -

UK – National AI Strategy[140]

EU – Proposed Artificial Intelligence Act[141]

USA – National Artificial Intelligence Initiative Act 2020[142]

China - Internet Information Service Algorithmic Recommendation Management Provisions (effective March 2022)[143]

Plainly, AI risk based regulation of behavioural advertising would be a paternalist intervention into consumer data protection, potentially marginalising notice and consent / choice frameworks. Yet, as suggested above, when based on based in legislation in democratic systems new regimes of this kind are potentially open to greater public accountability than regulatory and judicial principles-based rule

[136] UK Government Policy paper, Data: A new direction, 10 September 2021 https://bit.ly/3s7da2H
[137] Article 29 Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 6 February 2018 https://bit.ly/3ncbqCf; Ralf Poscher, 'Artificial Intelligence and the Right to Data Protection' Max Planck Institute for the Study of Crime, Security and Law Working Paper No. 2021/03 https://bit.ly/3LMD6br https://bit.ly/3Ku5Q7b
[138] California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments – Part One, 8 November 2021, https://bit.ly/3KlOKcQ
[139] Alicia Solow-Niederman, 'Information Privacy and the Inference Economy', Northwestern University Law Review, Forthcoming, 2022 https://bit.ly/35iTNuf
[140] United Kingdom, National AI Strategy, September 2021 https://bit.ly/3KwvZU8; CMA, Ofcom, ICO and FCA, 'The benefits and harms of algorithms: a shared perspective from the four digital regulators' 28 April 2022 https://bit.ly/37XfYrW

[141] Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) COM/2021/206 final https://bit.ly/33zXWtg; BEUC, Regulating AI to Protect the Consumer: Position Paper on the AI Act https://bit.ly/3LRSao8
[142] National Artificial Intelligence Initiative Act 2020 https://bit.ly/3kCq2ce; Spandana Singh, Regulating Platform Algorithms - Approaches for EU and U.S. Policymakers, New America – Open Technology Institute 1 December 2021 https://bit.ly/3GKdhG0; Alex Engler, 'The EU and U.S. are starting to align on AI regulation', Brookings, 1 February 2022 https://brook.gs/3KJ49D1
[143] Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 2022 https://stanford.io/3nLcA84; Helen Toner, Paul Triolo and Rogier Creemers, 'Experts Examine China's Pioneering Draft Algorithm Regulations' DigiChina, 27 August 2021 (*Internet Information Service Algorithmic Recommendation Management Provisions*) https://stanford.io/3IbT6kA; Matt Sheehan, China's New AI Governance Initiatives Shouldn't Be Ignored, Carnegie Endowment for International Peace, 4 January 2022 https://bit.ly/3tEPh3C

making. Nonetheless, public participation in policy and law making regarding digital technologies is at present weak. Although many consumers are fully aware that their lives are changing through constant technological and commercial innovations, the avenues for effective participation in decision making are not as apparent. In the UK, there is evident concern by policy makers that the harms and benefits of artificial intelligence are best considered and decided with a minimum of direct public participation.[144] While that approach may appear more efficient, the regulation of artificial intelligence is likely to have a major impact on the home and working lives of citizens, including personalised services, devices and environments that integrate advertising services. There are, consequently, key questions that require better public knowledge[145] and participation if the choices being made are to have public legitimacy.[146] These include -

- when is personalisation (tracking, profiling and targeting) acceptable?
- What sort of personalised services should be left to personal choice and what should be prohibited by law?
- For personalised services open to personal choice, how can those individual decisions be made informed and meaningful?
- Should people be allowed to exchange personal data for services?
- More specifically, if advertising is necessary to pay for new digital services low income people cannot afford, is it acceptable to combine personalised service data for behavioural advertising purposes?

For data protection regulators, the advent of AI risk regulation will aid but also complicate the regulation of behavioural advertising. There is a significant risk of gaps opening between rights based notice and consent frameworks in consumer data protection and new harms based duties for AI developers and operators[147] Part of the solution may, however, also lie in greater public participation in data protection regulatory decision making, which would help to provide greater public legitimacy for fairness and other principles based innovations to address the risks of AI driven harms. Public

[144] Archie Drake, Perry Keller, Irene Pietropaoli, Anuj Puri, Spyros Maniatis, Joe Tomlinson, Jack Maxwell, Pete Fussey, Claudia Pagliari, Hannah Smethurst, Lilian Edwards & Sir William Blair (2021) Legal contestation of artificial intelligence-related decision-making in the United Kingdom: reflections for policy, International Review of Law, Computers & Technology, DOI: 10.1080/13600869.2021.1999075

[145] Hacker, Philipp and Passoth, Jan-Hendrik, Varieties of AI Explanations Under the Law. From the GDPR to the AIA, and Beyond (August 25, 2021).https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3911324\

[146] Marina Micheli, Marisa Ponti, Max Craglia and Anna Berti Suman, 'Emerging models of data governance in the age of datafication', Big Data & Society (2020) July–December: 1–15 https://bit.ly/35tiPEc

[147] Jenny Berholm, 'The GDPR and the Artificial Intelligence Regulation – it takes two to tango?' Knowledge Centre – Data and Society, November 2021 https://bit.ly/3fC6qmf; Gloria González Fuster and Michalina Nadolna Peeters, 'Person identification, human rights and ethical principles', EPRS European Parliamentary Research Service, December 2021 https://bit.ly/3ruOrDJ

consultation exercises structured to go beyond interested business or civil society organisations could be usefully explored.

Across the four jurisdictions under discussion, there are currently only limited opportunities for representative or class actions to claims remedies for breaches of data protection law. The GDPR leaves this question to EU member states, who have responded with cautious experimentation or refusal.[148] No class or representative rights have been created as part of data protection law in the UK[149] or in new state level consumer privacy laws in the United States[150] or in China's new national data protection law.[151] On the other hand, the development of new public transparency duties for major online platform providers[152] could develop into a major avenue for changing information governance through research and public debate supported through government funding.[153]

Where representative or class action rights do exist in relation to consumer data protection law, or when advancing complaints to data protection regulators, privacy activist organisations face a problem of apparent self-appointment in pushing for a re-construction of online advertising and the personalisation of services. For the public, these endeavours may appear as arguments over regulatory and technical details, even though issues of enormous consequence are being decided. As noted above, advocating solutions, such as 'bright patterns' leaves open the objection that they are gaming consumer ignorance for their wider goals.[154] The answer here may also lie in more public engagement that goes beyond public education.

---

[148] But see, Directive 2020/1828 of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, 25 November 2020 https://bit.ly/3t58N7A; Case C-319/20 *Meta Platforms Ireland*, European Court of Justice (CJEU) 28 April 2022 https://bit.ly/3scup1V

[149] Matt Getz and Kimmie Fearnside, 'Lloyd v Google: U.K. Supreme Court on Representative Actions for Personal Data Breach Claims' European Data Protection Law Review Volume 7 (2021), *Issue 4*

[150] But see, Illinois Biometric Privacy Act - Woodrow Hartzog, 'BIPA: The Most Important Biometric Privacy Law in the US?', in Regulating Biometrics: Global Approaches and Urgent Questions, ed. Amba Kak (AI Now 2020) https://bit.ly/3JIisrd

[151] Article 70 of the PIPL empowers Consumer Association, Procuratorate, or institutions designated by the Cyberspace Affair authorities to file class action lawsuits against illegal data processing that affects multiple individuals or the unknown public – See Annex Two

[152] David Nosák, 'The DSA Introduces Important Transparency Obligations for Digital Services, but Key Questions Remain', Center for Democracy and Technology, 18 June 18 2021 https://bit.ly/3LRhydS ; Electronic Frontier Foundation (EFF) and ACLU California Action Comments, California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments – Part One, 8 November 2021, https://bit.ly/3KlOKcQ 'arguing for '[a] full right to know, which includes not only who companies have shared information with, but also what information has been shared. When it comes to protecting our own privacy, consumers are at a huge disadvantage. Companies know what they collect, how they use it, and who they share it with. Consumers usually do not.'

[153] European Commission, Emerging models of data governance and the politics of data, Digitranscope Project Joint Research Centre, 2020 https://bit.ly/3fSEGKp

[154] Network Advertising Initiative Comments, California Privacy Protection Agency, Preliminary Rulemaking Activities: Written Public Comments – Part Four, 8 November 2021, https://bit.ly/352x3Pd

Annex One

United States - Consumer data protection legislation

Perry Keller
Reader in Media and Information Law
King's College London

In the United States, laws governing 'consumer data protection' issues are divided between federal and state laws and, within both those levels, are sectoral rather than comprehensive. In this respect, 'data privacy' legislation in the United States is unlike the UK, EU and China in not having a primary, comprehensive data privacy statute. Some of the numerous bills before Congress proposing new data privacy legislation envisage a comprehensive consumer data privacy statute, but not a comprehensive data protection applicable to all processing of personal data.

1. U.S Federal laws relating to consumer data protection

Background reading

Neil Richards, Andrew Serwin and Tyler Blake, **'Understanding American Privacy'** in Gloria González Fuster, Rosamunde van Brakel and Paul De Hert (eds.), *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics*, Edward Elgar (2018) https://bit.ly/3enFDuq

Chris Hoofnagle, **Federal Trade Commission Privacy Law and Policy** (Cambridge University Press, 2016) - Chapter 6 Online Privacy https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2800276

Woodrow Hartzog and Neil Richards, **Privacy's Constitutional Moment and the Limits of Data Protection** (2020) 61 *Boston College Law Review* 1687 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441502

United States Constitution

The U.S. Constitution governs acts of the federal government and acts of state governments as required by the Fourteenth amendment, notable including the Bill of Rights (the first ten amendments) but does not directly govern the actions of private parties.

The Fourth Amendment restricts the search and seizure powers of state law enforcement agencies, including electronic data collection and further processing for surveillance purposes. There is, however, no positive Constitutional duty for the state to legislate to protect citizens from the privacy invasive acts of other private parties.

The First Amendment Constitutional right to freedom of speech is expansively interpreted by the courts and limits the powers of the federal and state governments to legislate to protect privacy interests that infringe the liberty to share information that is in the public domain or is of public interest ('newsworthy'). The Supreme Court's decision in *Sorrell* v. *IMS Health Inc* (below) is a significant demonstration of the potential impact of the First Amendment on U.S. data protection legislation.

U.S. Constitution, First Amendment (Adopted 1791)

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the **freedom of speech, or of the press;** or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

***Sorrell* v. *IMS Health Inc.*,** 564 U. S. 552, 566 (2011) United States Supreme Court https://www.law.cornell.edu/supct/pdf/10-779P.ZO

Gautam Hans, **No Exit: Ten Years of 'Privacy vs. Speech' Post-Sorrell** (2021) *Washington University Journal of Law and Policy*, Vol. 65, 2021 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3740346

Spencer, Shaun B., **Two First Amendment Futures: Consumer Privacy Law and the Deregulatory First Amendment** (2020). Michigan State Law Review, Vol. 2020, No. 3, 2020, Available at SSRN: https://ssrn.com/abstract=3769385

Federal legislation concerning consumer data protection

The primary federal regulatory powers concerning consumer data protection are found in the section 5(a) of the Federal Trade Commission Act. When businesses act deceptively (e.g. do not abide by their published privacy notices) the FTC may seek to impose sanctions for such deceptive acts (FTC fines must be imposed only with court approval) The FTC relies on the unfairness basis less often than the deceptive basis.

Section 5(a) of the FTC Act, 15 U.S.C. § 45(a)
https://www.law.cornell.edu/uscode/text/15/45

(a) Declaration of unlawfulness; power to prohibit unfair practices;

(1) Unfair methods of competition in or affecting commerce, and **unfair or deceptive acts or practices in or affecting commerce**, are hereby declared unlawful.

(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except ... ... from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

The U.S. Supreme Court's 2021 decision in ***AMG Capital Management, LLC v. FTC*** drastically limited the FTC's ability to seek, or a court to award, equitable monetary relief such as restitution or disgorgement.

In its annual **Report to Congress on Privacy and Security** (September 2021 - https://bit.ly/3p3hUo0) the FTC set out its enforcement priorities –

Integrating consumer protection and competition concerns when addressing overlapping dayta privacy and competition problems in digital markets.

Expanding remedies, including
- Providing notice to harmed consumers.
- Obtaining monetary remedies for harmed consumers.
- Obtaining non-monetary remedial relief for consumers.
- Not allowing companies to benefit from illegally collected data.

Focusing on dominant digital platforms to ensure limited FTC are focused on the most egregious practices and cases against major players in the marketplace in order to have a broader impact

Expanding understanding of algorithms to deepen our understanding of the consumer protection and competition risks associated with algorithms and to expand upon the guidance

that we have provided to businesses on using algorithms and AI truthfully, fairly, and equitably.

Federal Trade Commission, Division of Advertising Practices https://bit.ly/3GPxJED

As an example of a major FTC enforcement action related to behavioural advertising, see

United States of America v. Facebook, Inc., United States District Court for the District Of Columbia, 24 July 2019, Case No. 19-cv-2184

Complaint for Civil Penalties, Injunction, and other Relief - https://bit.ly/2WskupT

1. Plaintiff brings this action against Defendant Facebook, Inc. ("Facebook") under **Sections 5(a)** and (l) and 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 45(a) and (l) and 56(a)(1), to obtain civil penalties, an injunction, and other equitable relief for violations of a 2012 order previously issued by the Federal Trade Commission ("FTC" or "Commission") for violations of Section 5(a) of the FTC Act. See Exhibit A, *In re Facebook, Inc*., C-4365, 2012 FTC LEXIS 135 (F.T.C. July 27, 2012) (Decision and Order) ("Commission Order" or "2012 Order"). This action seeks to hold Facebook accountable for its failure to protect consumers' privacy as required by the 2012 Order and the FTC Act.

Stipulated Order for Civil Penalties, Injunction, and other Relief - https://bit.ly/2U3roAx

Michel Protti, Chief Privacy Officer, Facebook, **Final FTC Agreement Represents a New Level of Accountability for Privacy,** April 23, 2020 https://about.fb.com/news/2020/04/final-ftc-agreement/

Petitions to the FTC for investigations or rule making regarding behavioural advertising, see for example -

Accountable Tech - **Petition to the FTC for Rulemaking to Prohibit Surveillance Advertising**, 27 December 2021 https://bit.ly/3BEXo23

FTC Invitation for comments, Federal Register Vol. 86, No. 245 Monday, December 27, 2021 Proposed Rules https://bit.ly/3BAwTe8

Children's Online Privacy Protection Act (COPPA) is a notice and consent based federal regulatory regime for the protection of children as online service users, which is enforced by the FTC under s.5 of the FTC Act –

Children's Online Privacy Protection Act (COPPA) 15 U.S. Code, Chapter 91 https://www.law.cornell.edu/uscode/text/15/chapter-91

FTC – Children's Online Privacy Protection Rule
Code of Federal Regulations, PART 312
https://bit.ly/2syMdWP

Bills currently before Congress relating to consumer privacy protection include -

H.R.6416 **- Banning Surveillance Advertising Act of 2022** https://bit.ly/3LIdCMm

S.3627 - **Data Elimination and Limiting Extensive Tracking and Exchange Act (DELETE Act)** https://bit.ly/3HkvV7b

2. U.S. state laws relating to consumer data protection

IAPP Resource Center, **U.S. State Privacy** https://iapp.org/resources/topics/us-state-privacy/

NCSL - **National Congress of State Legislatures,** 2021 Consumer Data Privacy Legislation, 27 December 2021 https://bit.ly/3sReEgk

Uniform Law Commission, **Uniform Personal Data Protection Act,** July 2021 https://bit.ly/3sbjXIF

California Consumer Privacy Act

California Consumer Privacy Act (**CCPA**) 2018 https://bit.ly/390mxo1

The CCPA came into effect on 1 January 2020 - Enforcement commenced 1 July 2020

The CCPA was amended by the **California Privacy Rights Act** (CPRA), which was adopted in November 202 by public vote – Proposition 24

Annotated version of CCPA to show CPRA changes - https://bit.ly/3p7YWMT

The CPRA will come into effect on 1 January 2023

California Consumer Privacy Act Regulations https://bit.ly/3bKC9R8

Article 1 - General Provisions

§ 999.300. Title and Scope.

(a) This Chapter shall be known as the California Consumer Privacy Act Regulations. It may be cited as such and will be referred to in this Chapter as "these regulations." These regulations govern compliance with the California Consumer Privacy Act and do not limit any other rights that consumers may have.

(b) A violation of these regulations shall constitute a violation of the CCPA and be subject to the remedies provided for therein.

California Consumer Privacy Act (CCPA) Current Rulemaking Activities
https://oag.ca.gov/privacy/ccpa/current

On January 26, 2021, the Department of Justice filed with the Office of Administrative Law (OAL) proposed amendments to the CCPA regulations. The amendments address withdrawn regulations from previous rulemaking documents that were submitted to and approved by OAL.

California Consumer Privacy Act FAQs https://oag.ca.gov/privacy/ccpa

The California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

Businesses are required to give consumers certain notices explaining their privacy practices. The CCPA applies to many businesses, including data brokers

California Privacy Protection Agency https://cppa.ca.gov

The California Privacy Rights Act established a new agency, the California Privacy Protection Agency (CPPA), and vested it with the "full administrative power, authority and jurisdiction to implement and enforce the California Consumer Privacy Act of 2018." The Agency's responsibilities include updating existing CCPA regulations and adopting new regulations.

Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21) September 22, 2021 https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf

1. Processing that Presents a Significant Risk to Consumers' Privacy or Security: Cybersecurity Audits and Risk Assessments Performed by Businesses
2. Automated Decision making
3. Audits Performed by the Agency
4. Consumers' Right to Delete, Right to Correct, and Right to Know
5. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information
6. Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information
7. Information to Be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)
8. Definitions and Categories
9. Additional Comments

California Privacy Protection Agency, Preliminary Rulemaking Activities: **Written Public Comments – Part One**, 8 November 2021, https://bit.ly/3KlOKcQ

California Privacy Protection Agency, Preliminary Rulemaking Activities: **Written Public Comments – Part Two**, 8 November 2021, https://bit.ly/3nApkOV

California Privacy Protection Agency, Preliminary Rulemaking Activities: **Written Public Comments – Part Three**, 8 November 2021, https://bit.ly/3Id6QM6

California Privacy Protection Agency, Preliminary Rulemaking Activities: **Written Public Comments – Part Four**, 8 November 2021, https://bit.ly/352x3Pd

3. Other California state laws relating to consumer data protection

Constitution of the State of California

Article I - Declaration of Rights

Section 1 All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and **privacy**.

(Article 1 adopted 1879, Section 1 was added in 1974 by Proposition 7)

California Online Privacy Protection Act (CalOPPA) 2002 https://bit.ly/3sTs2AF

Businesses that collect any personally identifiable information (PII) from an online web / mobile app consumer residing in California (including name, address, email address, phone number, social security number) must make privacy policy disclosures to potential consumers

California Data Security Breach Notification Law (2002) https://bit.ly/3cyA5uy

California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person.

Shine the Light Law 2003 https://bit.ly/2OnoarD

The "Shine the Light" law creates rights for individuals to know how businesses sell their personal information.

California Financial Information Privacy Act (CalFIPA) 2003 https://bit.ly/3rOADmB

CalFIPA requires financial institutions to provide California consumers notice and choice about regarding the sharing of personal financial information.

4. Other significant U.S. state laws relating to consumer data protection

Virginia Consumer Data Protection Act 2021 (effective 1 January 2023) https://bit.ly/3sTuyXD

Virginia Consumer Data Protection Act Work Group 2021 Final Report https://bit.ly/3M0nAci

Colorado Privacy Act 2021 (effective 1 July 2023) https://bit.ly/3LRs4le

Utah Consumer Privacy Act 2022 (effective 31 December 2023) https://bit.ly/3rZvyKh

Illinois Biometric Information Privacy Act (BIPA) 2008 740 ILCS 14 et seq. https://bit.ly/3sZCcQg

Illinois Biometric Information Privacy Act FAQs http://bit.ly/2BiARau

Annex Two

China - Consumer related data protection laws and regulations

Dr. Li Yang
Research Associate / 博士后研究员
King's College London

This annex aims to provide a comprehensive overview of the major laws and regulations concerning personal information protection and online advertising in China. Apart from the high-profile Personal Information Protection Law, there are a large number of rules regarding AdTech companies and their online advertising business in the Chinese legal system, spreading across not only different law areas but also varying levels of legal authority. For the sake of clarity, this annex divides the related Chinese laws and regulations into three parts according to their authority levels, namely, national laws, administrative and ministerial regulations, and non-binding guidelines and national standards. [155] Within each part, the documents are arranged in reverse chronological order with the latest (and usually the most relevant) ones at the beginning.

Part I: National Law

1. Personal Information Protection Law (《个人信息保护法》)[156]

In August 2021, the Standing Committee of the National People's Congress of China (hereafter, the SC-NPC) enacted the long-anticipated Personal Information Protection Law (the PIPL), China's first-ever comprehensive data protection law. The PIPL came into effect from 1st November 2021. Since then, the PIPL becomes the most important piece of legislation for regulating the AdTech industry and online advertising in the Chinese legal system.

Generally speaking, many common elements of data protection legislation, such as the legal basis for processing[157], data protection principles[158], data subject rights[159], obligations of data controllers on data security and incident reporting[160], and rules for international transfer of data[161], can all be found

[155] See details about complex hierarchy in the Chinese legal system: Perry Keller, 'Sources of order in Chinese law.' *The American Journal of Comparative Law* 42, no. 4 (1994): 711-759.
[156] See the full text of the PIPL at: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml. A non-official English translation is available at https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.
[157] Ibid, Art 13.
[158] Ibid, Arts 5-9 and Art 19.
[159] Ibid, Arts 44-50.
[161] Ibid, Art 38-43.
[161] Ibid, Art 38-43.

in the Chinese PIPL. Moreover, like the EU GDPR, the PIPL has a rather broad material scope of application, covering both identified and identifiable elements of personal information and governing the entire information processing lifecycle.[162]

Regarding the AdTech companies, the PIPL contains rules for almost every key phase of data processing for their online advertising, in particular, data collection, data sharing, and automated decision-making. Specifically, Art 13 of the PIPL sets out seven legal bases for personal information processing, including consent, contract, legal duties and obligations, public health emergency or other emergent circumstances alike, journalistic report in the public interest, reasonable use of public data, and other circumstances specified by laws and administrative regulations. While this creates a possibility for AdTech companies to utilise the legal basis of contract in their online advertising operations, the common practice in the Chinese AdTech industry is still to obtain consent from the individual users. This is probably because before the enactment of the PIPL consent was the only valid basis for personal information processing in Chinese law.

Where consent is used as the legal basis, such consent must be 'fully informed, freely given, and unambiguous' (Art 14); and the data controller must 'truthfully, accurately, and completely' inform the individual of several matters specified in Art 17, including the name, contact details of the data controller, the purpose and method of data processing, the type of data processed, data retention period, the methods and procedures for individuals to exercise their rights, etc. Moreover, the data controller must provide the individuals with a convenient way to withdraw their consent (Art 15) and must not decline the provision of services or products because the individuals withdraw their consent unless such information is necessary for the provision of the services or products (Art 16). In addition, where sensitive personal information is to be processed, such as biometric and religious information, medical and health record, financial account, personal track and trace, and personal information of minors under 14 years of age, etc., the data controller must inform the individuals of the necessity of such processing and possible impact on the individuals' rights and interests and obtain 'separate consent' from the individual. (Art 28-30). Other laws and administrative regulations may impose additional requirements for the processing of certain sensitive data, such as 'written consent' or 'administrative license'. (Art 29 and Art 32).

The PIPL also includes several rules concerning data sharing—an essential but very perturbing part of processing in online advertising. According to the PIPL, when providing personal information to a third party, the data controller must inform the individual of the name and contact information of the third-party recipient, the purpose and method of processing, and the type of personal information to be transferred and obtain separate consent from the individual. If such information transfer is due to corporate mergers, acquisitions, split-up, dissolution, insolvency etc, the individual's consent is not required, but the data controller still needs to inform the individual of the above-mentioned matters; and the third party information recipient shall only process personal information within the scope

[162] Ibid, Art 4.

stated in the data provider's privacy notice, and must inform and re-obtain consent from the individual when it changes the purpose or method of information processing.

Noteworthy, the PIPL, like the EU GDPR, makes a distinction between the data controller and the data processor. The above-mentioned requirements for data sharing with third parties, therefore, do not apply to the data controller and data processor relationship. According to the PIPL, data controllers may entrust others to process personal information for them by concluding an entrust agreement. The entrusted body (i.e., data processor in the GDPR' s term) must process personal information strictly following the agreement, and the data controller is responsible for supervising their information processing. If the entrusting contract does not take effect, becomes void, has been cancelled or terminated, the entrusted person shall return the personal information to the controller or delete it, and must not retain it (Art 21). By contrast, where two or more bodies jointly decide the purpose and method of personal information processing, they will be considered as joint data controllers and be held jointly liable for damages created for the individuals. The rights and obligations set out in the contractual agreement between the data controllers do not affect the individual's rights against them (Art 21). In addition, both sharing personal information with a third party and entrusting others to process personal information are among the circumstances that a Personal Information Protection Assessment (PIPA) are explicitly required (Art 55 (3)).

Regarding automated decision-making, the PIPL imposes four major obligations on the data controller[163]: first, the data controller must ensure the transparency of automated decision-making, and that the result of the automated decision-making is fair and just for the individuals. Unreasonable differential treatments, such as price discrimination, are expressly prohibited. Second, where automated decision-making is used for pushing up information or advertisements, the data controller must provide a non-personalised option or a convenient way for the individual to object. Third, if the automated decision-making has a significant impact on the individuals, the individuals have the right to ask the data controller to explain and to reject the decision made solely through the automated decision-making method. In addition, the PIPL also includes automated decision-making, together with processing of sensitive personal information, entrusting others to process personal information or sharing personal information with a third party, and international transfer of personal information in the list of circumstances that the Personal Information Protection Assessment (PIPA) is mandatory[164]

There are three major enforcement mechanisms under the PIPL, namely, administrative enforcement, criminal punishments and civil law remedies. The PIPL grants the supervisory authorities the power to impose an administrative penalty of up to 50 million RMB or 5 % of annual turnover, in addition to rectification notice, official warning, confiscation of illegal gain, suspension or termination of non-compliant apps, and revocation of business license (Art 66). This is a significant boost of penalty

[163] Ibid, Art 24.
[164] See the full list of the circumstances that require PIPA in Art 55. The requirements of the PIPA are stipulated in Art 56.

power compared to the previous Chinese laws and regulations concerning personal information protection. Criminal punishments have been the most relied-on mechanism to enforce data protection in China.[165] Art 71 of the PIPL, not surprisingly, reacknowledges the important role of criminal law in China's data protection regulation. Regarding civil law remedies, the Chinese Civil Code 2020 had given individuals the right to request legal remedies via lawsuit when their rights/interests to personal information protection and/or privacy are infringed. Art 69 and Art 70 of the PIPL further strengthen the existing judicial enforcement mechanism by respectively reversing proof burden for civil law cases concerning infringements on individuals' personal information, and empowering Consumer Association, Procuratorate, or an institution designated by the Cyberspace Administration of China (CAC) to file class lawsuits against illegal information processing that affect many individuals.

The PIPL also has many obvious weaknesses. Most notably, the competence of administrative enforcement remains scattered under the PIPL (Art 60). Unlike the UK and EU countries that have established specialised and independent data protection authorities, the supervisory competence in the Chinese data protection regime is shared by different administrative authorities according to their governing industries and fields.[166] The representative lawsuit clause (Art 70) and the gatekeeping obligation of large platforms (Art 58) seem to be introduced to alleviate the regulatory gaps caused by the scattered supervisory competence. According to the 'Typical Cases of Personal Information Protection Class Suits handled by Procuratorates' released by the Supreme Procuratorate in 2021, local procuratorates have been increasingly undertaking a role to urge competent administrative authorities to exert their supervision and enforcement power in personal information protection. [167] However, the efficiency of the innovative measures is yet to be seen.

What is more, the rules in the PIPL (74 clauses in total) are rather abstract and broadly stated. Admittedly, a series of national standards and non-binding guidelines regarding personal information protection in general and related issues have been enacted or drafted in recent years.[168] If widely endorsed by the supervisory authorities and courts, these voluntary guidelines might significantly

[165] The website of Shanghai High Court shows that within the municipality of Shanghai alone, there were142 cases and 278 individuals being prosecuted under Article 253 (a) from the enactment of the Seventh Amendments to Criminal Law in 2009 to 30th April 2015 (See: http://shfy.chinacourt.org/article/detail/2016/07/id/2001638.shtml) According to the latest statistics of the Supreme Court, from June 2017 to June 2021, courts nationwide received 10,059 new criminal cases concerning citizens' personal information, concluded 9,743 cases, 21,726 people were sentenced to effect, and 3,803 defendants were sentenced to more than three years in prison. (See: https://www.court.gov.cn/fabu-xiangqing-315831.html).

[166] This, however, is not exclusive to data protection regulation, but a long-standing problem in Chinese law. More details see: Angela Huyue Zhang, 'Agility Over Stability: China's Great Reversal in Regulating the Platform Economy' (July 28, 2021). Harvard International Law Journal, Vol. 63, No. 2, 2022 (forthcoming) https://ssrn.com/abstract=3892642.

[167] See: https://www.spp.gov.cn/spp/xwfbh/wsfbt/202104/t20210422_516357.shtml#2. More recently, on 27 February 2022, the Supreme Procuratorate published an article on its official website, stating that procuratorates nationwide had handled over 2,000 class action cases concerning personal information protection i 2021. Many of the cases were regarding mobile apps' misuse of personal information. See: https://www.spp.gov.cn/spp/xwfbh/wsfbh/202202/t20220227_545967.shtml.

[168] See details in Part III.

improve the certainty of the PIPL. However, before that happened, there are still huge uncertainties regarding how the abstract rules in the PIPL will be interpreted and implemented in practice.

2. Data Security Law (《数据安全法》)[169]

Data Security Law (hereafter, the DSL) was adopted by the SC-NPC on 10 June 2021 and became effective from 1st September 2021. The DSL is another significant piece of national law concerning data protection adopted by the SC-NPC in 2021. The DSL together with the PIPL and Cybersecurity Law, are often referred to as the three major pieces of legislation for data protection in China.[170] The material scope the DSL, however, are much broader than the PIPL. Specifically, the PIPL applies to natural persons' personally identified or identifiable information,[171] whereas the DSL governs the processing of 'any data that is recorded in digital or other forms'.[172] In other words, AdTech companies not only need to comply with the PIPL in their personal information processing activities, but also must observe the DSL in the processing of both personal and non-personal data.

The DSL stipulates several security requirements on the processing of (both personal and non-personal) data. Most notably, the DSL introduces a 'data categorisation and classification protection system' which classifies data into three main categories, i.e., state critical data, important data, and ordinary data. For the first two categories, enhanced data security obligations will apply, such as the establishment of a specialised data security body and officer (Art 27), regular risk assessment and reporting to the supervisory authorities (Art 30), and increased restriction on international data transfer (Art 31 and Art 25). However, like the PIPL, the implementation and practical impact of the rules remain to be seen due to the generic feature of the clauses. It is not yet clear if and to what extent of AdTech companies' databases will be regarded as important data or even state critical data, and thus are required to undertake the enhanced security responsibilities.

What is more, Art 28 of the DSL requires that any data processing activities and developments of new data technologies must respect the ethical values of society and promote the well-being of people. This requirement seems to be a major legal basis of the new Algorithm Provisions, which impose a series of obligations on algorithm operators to respect and preserve social, business, and professional ethics (see details in Part II).

[169] See the full text of the DSL: http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml. A non-official English translation is available at https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/.
[170] For example, see https://www.dataguidance.com/notes/china-data-protection-overview.
[171] See Art 2 and Art 3 of the PIPL.
[172] See Art 3 of the DSL.

3. **Civil Code** （《民法典》）[173]

The Civil Code was adopted by the National People's Congress（NPC) in 2020 and took effect from 1st January 2021. Before the promulgation of the Civil Code, claims against infringements on individuals' personal information were often regarded as or confused with the claim concerning the right to privacy which only governs public disclosure of private information, a much narrower scope of personal information and information processing activities. The Civil Code expressly differentiates the right to privacy and individuals' civil right/interest to personal information protection (Art 111), defines the scope of personal information (Art 1034 (1)) and stipulates several rules specifically for personal information protection (Arts 1035 – 1038). Consequently, behaviours like failing to publicise personal information processing rules, failing to notify individuals of the purpose, method, and scope of information processing, failing to obtain consent from the individuals, processing personal information in violation of the agreement with the individuals (Art 1035), providing personal information to a third party without the individual's prior consent (Art 1038) etc. may all be regarded as infringements on the individual's legal interest/right to personal information protection and liable under the Civil Code.

Nevertheless, the civil lawsuit as the major way for the aggrieved individuals to obtain legal remedies in China entails several problems: firstly, compensation, the most effective legal remedy, is merely available for the individuals who have suffered physical damage, monetary loss, or 'severe mental damage' as the result of the personal information misuse.[174] Given the high costs of lawsuits and the low chance to obtain any compensation, civil lawsuits can only be a game affordable by a small group of people who have enough time, financial recourses, and really care about their personal information. Secondly, very high proof standards and burden. For example, in the passing years, several civil lawsuits regarding personal information leaks were launched, but most were declined by the court. A major reason is that the data subjects were not able to prove that the personal information was 'definitely' leaked by the defendant data controller, not others.[175]

The PIPL, as mentioned above, has responded to the problems. Art 69 of the PIPL changes the normal situation in which the plaintiff must prove the facts and establish causation, and instead requires the data controller to prove it has no fault in its personal information processing. Art 70 empowers Consumer Association, Procuratorate, or institutions designated by the Cyberspace Affair authorities to file a class lawsuit against illegal data processing that affects multiple individuals or the

[173] The full text of the Civil Code can be found at http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml. An official English translation is available at http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf.

[174] Ibid, Art 1179, Art 1182, and Art 1183.

[175] For example, see Zheng Yang V Tianjin Airline Co., Ltd, and Zhejiang Taobao Co., Ltd, Court of Dongli District, Tianjin City, No. 1720 of 2014 (郑洋与天津航空有限责任公司，浙江淘宝网络有限公司隐私权侵权纠纷案，天津市东丽区法院，（2014）丽民初字第 1720 号). Wang Jingsu V Beijing City branch of China Telecommunications Co., Ltd, and Wang Tao, No. 2 Intermediate Court of Beijing City, No.194 of 2017(王景素与中国电信北京分公司，王涛隐私权纠纷案，（2017）京 02 民终字 194 号).

unknown public.[176] Hence, we are expecting to see improvements in the civil enforcement mechanism for personal information protection in the coming months and years as the PIPL is implemented.

4. E-commerce Law (《电子商务法》)[177]

E-commerce Law was passed by the SC-NPC in August 2018 and came into effect from 1st January 2019. E-commerce Law, as the title indicates, applies to electronic commerce—defined as 'any business activities related to selling goods and services via information networks',[178]conducted within the territory of China. Financial products/services, and services regarding news, publishing, audio and visual programmes, culture and other contents etc. are expressly excluded from the scope of application.[179]In other words, E-commerce Law applies only to AdTech companies that conduct e-commerce, but not those that provide financial services, news, audio, videos contents etc.

Expressly aiming to protect the legitimate rights and interests of different parties in e-commerce businesses, maintain market order and promote sustainable development of e-commerce in China (Art 1), the E-commerce Law introduced several rules to regulate e-commerce operators and platforms and to protect consumers and other stakeholders (e.g., intellectual right holders[180]). These include several clauses for the protection of users' personal information. For instance, Art 18 obliges e-commerce operators, when providing consumers with search results for products and services based on their hobbies, preferences, spending habits and other personal characteristics, to offer consumers non-personalised options. Art 24 requires e-commerce operators to clearly indicate the methods and procedures for the access, rectification, and deletion of personal information, and account cancellation, prohibiting e-commerce operators from setting up unreasonable conditions for users to exercise the above-mentioned rights. Likewise, Art 32 and Art 33 require e-commerce platforms to follow the principles of transparency, fairness, and justice, make and publicise platform service agreements and trade rules, ensuring the protection of consumer rights and interests including those relating to their personal information. Art 34 obliges e-commerce platforms to publicly solicit comments from related parties before revising the platform service agreements and trade rules and to continue to undertake the original responsibilities where a party refuses to accept the revised contents and withdraws from the platform. Nevertheless, the relevance and importance of the E-commence Law in the protection of personal information have been significantly reduced nowadays, as the PIPL and the Civil Code are implemented.

---

[176] However, there is still controversy as to whether punitive compensation applies to personal information representative cases, and how the compensation awarded in the representative lawsuit should be allocated. See: 张新宝, 赖成宇: '个人信息保护公益诉讼制度的理解与适用', 国家检察官学院学报，2021 年第 5 期 .https://www.163.com/dy/article/GNQQNNF50530W1MT.html.
Also see a related news report: http://fzzfyjy.cupl.edu.cn/info/1035/13587.htm.
[177] The full text of the E-Commerce Law can be found at http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2018-08/31/content_2060827.htm. A non-official English translation is available at https://www.chinalawtranslate.com/en/p-r-c-e-commerce-law-2018/.
[178] Ibid, Art 2.
[179] Ibid.
[180] Ibid, Art 41-45 and Art 84.

5. **Advertising Law** (《广告法》)[181]

Advertising Law (hereafter, the AL) was adopted by the SC-NPC in 1994 and then revised respectively in April 2015 and October 2018. The AL is a major national law regulating the advertising industry and the conduct of advertisements in China. The focus of the AL, however, is on the regulation of advertisements' content (e.g., must not advertise for tobacco, drugs, medical devices etc.) and form (e.g., must not include potentially misleading expressions or pictures; endorsers must not endorse and advertise any products/services that they haven't used themselves).

There are a few clauses specifically for the regulation of online advertising in the AL. For instance, Art 43 prohibits any entities or individuals, without the individuals' consent or upon their request, to send advertisements to their homes, transport vehicles alike, or in the form of a digital message; where the advertisement is sent in the form of digital messages, it must clearly indicate the senders' real identification, and contact details, and to provide ways to decline future advertisements. Likewise, Art 44 requires that online advertisements must not affect people's normal use of the internet, and pop-up advertisements must provide an obvious close button and allow one-click close. Nevertheless, the legal consequence of violating the above rules is very minor for most AdTech companies: an administrative fine of up to 30,000 RMB (Art 63).

6. **Cybersecurity Law** (《网络安全法》)[182]

Cybersecurity Law was adopted by the SC-NPC in November 2016 and took effect from 1st June 2017. As a national law dedicated to the protection of cybersecurity, the CSL introduced several serious, and sometimes controversial,[183]measures for enhancing Internet security and combating cybercrimes. These include the graded protection system for network security (Art 21), compulsory security test and certification for certain network products (Art 23), and risk management for critical information infrastructure (Art 31-39) etc. By tightening up the overall network security, these measures may have a collateral effect on improving the protection of personal information in China.

The CSL also contains some clauses for the protection of individuals' personal information. For instance, Art 40 imposes a duty for the network operators to keep users' information confidential; Art 41 stipulates the principles of lawfulness, legitimacy, and necessity, as well as the requirements on the publication of data processing rules and the obtaining of data subject's consent; Art 42 sets out requirements on data security and incident reporting, as well as the conditions for providing personal

[181] The full text of the AL can be found at http://www.npc.gov.cn/zgrdw/npc/xinwen/2018-11/05/content_2065663.htm. A non-official English translation is available at https://www.hongfanglaw.com/wp-content/uploads/2019/10/Advertising-Law-of-the-Peoples-Republic-of-China-2018-AmendmentEnglish.pdf.
[182] The full text of the CSL can be found at http://www.cac.gov.cn/2016-11/07/c_1119867116.htm. A non-official translation is available at https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.
[183] For example, compulsory real identification registration for all internet and telecommunication users (Art 24), a vague and potentially broad obligation on internet firms to provide technical support and assistance to police and national security organs (Art 28) and the requirements for internet platforms to monitor and manage information published by their users (Art 47).

information to others; Art 44 prohibits individuals and entities from stealing, acquiring personal information via illegal means, and illegally selling or providing personal information to others; Art 45 stresses the confidential duty of supervisory authorities and their staff. These rules, for the most part, are restated in a more systematic and refined manner by the newly enacted PIPL. As a result, the importance and relevance of the CSL for the protection of personal information in the Chinese legal system are now significantly reduced.

7. **Criminal Law** (《刑法》)[184]

There are three criminal offences relating to personal information protection in Chinese law. The most relevant offence to AdTech companies is 'infringement of citizens' personal information' provided by Art 253.1 of the Criminal Law. Art 253.1 punishes illegal acquisition, sale, and provision of citizens' personal information to others. According to an Interpretation jointly issued by the Supreme Court and Supreme Procuratorate in 2017, there are only two exemption circumstances to the criminal offence of providing personal information to others, i.e., consent has been obtained from the individual, or the personal information has been anonymized and not possible to recover.[185] It is therefore crucial for AdTech companies, in their business operations, to make and keep clear records of individuals' consent and adopt effective anonymous measures before providing information to a third party. In theory, this clause may also be used to punish AdTech companies that maliciously collect users' personal information beyond the scope stated in their privacy policies. Because many established national laws, such as the PIPL (Art 5) and Civil Code (Art 1035 (4)), have obliged data controllers to follow the principles of honesty and not to process personal information in violation of agreements with individuals. AdTech companies' excessive collection, in this respect, can be considered as the illegal acquisition of personal information and be punished by Art 253.1. Nevertheless, Chinese regulators have never applied the criminal offence in this way. Instead, as shown in the Special Rectification Scheme on Apps (See Annex 3), Chinese regulators by far have been rather tolerant towards AdTech companies' excessive collection, imposing only mild penalty measures such as public naming, or temporarily removing apps from app stores.

namely, Art 253.1 infringing upon the Personal Information of Citizens, Art 285 intruding upon, illegally controlling a computer information system, or legally obtaining data in a computer information system, and Art 286.1. refusal to perform legal obligations regarding network security.

The second offence concerning personal information protection is 'intrusion upon, illegal control of a computer information system, or illegal acquisition of data from a computer information system' in Art 285 (2). This criminal offence was mainly used to punish malicious hackers who intrude upon, or

[184] See full text of the Chinese criminal law at http://www.npc.gov.cn/wxzlhgb/gb2021/202104/3a338df89b0a415481a9bf0571588f88/files/3d9248e01141484ead7d01b58958e0ae.pdf. A non-official English translation is available at https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/5375/138545/F-429698458/CHN5375%202020.pdf.
[185] https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml.

control others' computer information systems, or steal data from computer information systems. However, in recent years, it has also been used to criminalize data/ web scraping.[186] In other words, data/web scraping, a considerably common practice for start-up or small/medium AdTech companies to aggregate data,[187] bears a high risk of being punished under the Chinese Criminal law.

The third criminal offence, Art 286.1 refusal to fulfil legal obligations regarding network security, is rarely used in practice. This is due to its high threshold of application. Specifically, Art 286.1 can only be triggered if a network service provider refused to adopt remedial measures to address its information security-related misconducts after being ordered by a regulatory authority in the first place, and one of the three circumstances occur as a result, including dissemination of a large amount of illegal information, leakage of users' information with serious consequences, or loss of criminal evident with serious consequences. Not surprisingly, this criminal law provision has seldomly been used since the enactment of the Ninth Amendment to Criminal Law in 2015. Nevertheless, it is still a criminal offence that AdTech companies must be aware of.

8. **Consumer Protection Law** (《消费者权益保护法》)[188]

The Law on Protection of Customer Rights and Interests (hereafter, Consumer Protection Law) was originally adopted by the SC-NPC in 1993 and then amended respectively in August 2009 and October 2013. The 2013 amendments incorporated two clauses regarding the protection of consumers' personal information.

Specifically, Art 14 of the Consumer Protection Law explicitly states that consumers enjoy 'the right to have their personal information protected'. This was the first clause of the kind in the Chinese law, preceding the Civil Code[189] and its predecessor the General Principles of the Civil Law. [190] Art 29 of the Consumer Protection Law is a short but very comprehensive data protection clause. Its first paragraph stipulates the principles of lawfulness, legitimacy, and necessity, the requirements for business operators to publicise their information processing rules, notify the consumers of the purposes, means and scope of their personal information collection and use, and obtain consent from the consumers, as well as the prohibitions for business operators to collect or use information in violation of laws, regulations, or agreements with consumers. The second paragraph of Art 29 requires business operators and employees to keep consumers' personal information confidential, not to disclose, sell, or illegally provide it to others. Business operators are also required to take technical

[186] See https://www.chinacourt.org/article/detail/2020/01/id/4769105.shtml and https://www.allbrightlaw.com/CN/10475/3a742750e4a53fcc.aspx; https://cloud.tencent.com/developer/article/1547326.
[187] https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/data-scraping-considering-the-privacy-issues.
[188] The full text of the Consumer Protection law is available at http://www.npc.gov.cn/wxzl/gongbao/2014-01/02/content_1823351.htm. A non-official translation is available at https://www.chinalawtranslate.com/en/consumer-protection-law-including-2013-amendments/.
[189] The Civil Code, Art 111.
[190] See: http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-03/15/content_2018907.htm.The General Principles of Civil Law (《民法总则》) was adopted in 2017 and replaced by the Civil Code from 1 January 2021.

and other necessary measures to ensure information security and thereby prevent consumers' personal information from leakage and loss. In situations where information has been or might be leaked or lost, business operators shall immediately adopt remedial measures. [191] The last paragraph prohibit business operators from sending advertisements to consumers without their consent or upon their request, or where they have clearly refused it.[192]

These above rules have all been reiterated in more delicate and systematic ways by later legislation, such as the PIPL, the Civil Code and Advertising Law. Nevertheless, the Consumer Protection Law will remain important for data protection regulation in China. For one thing, the Consumer Protection Law has enabled Chinese Consumer Associations, a not-for-profit organization with hundreds of branches across different regions of China, to interfere in the cases concerning infringements on consumers' personal information. To be specific, Art 39(2) of the Consumer Protection Law provides consumers with the option to request Chinese consumer associations to mediate their dispute with business operators, whereas Art 47 empowers consumer associations to initiate a class action against 'behaviours infringing legal rights or interests of multiple consumers'. Neither provision is dedicated to the protection of consumers' personal information. However, by recognising consumers' right to personal information protection and incorporating the above data protection rules into its texts, the Consumer Protection Law has given Chinese consumer associations the legal competence to intervene in consumers' personal information protection cases, either in the capacity of a dispute mediator[193] or the representative of a class action.[194]

Part II. Ministerial Regulations

1. Provisions on the Management of Algorithmic Recommendation in Internet Information Service (《互联网信息服务算法推荐管理规定》)[195]

On 31 December 2021, the Cyberspace Administration of China (the CAC), the Ministry of Industry and Information Technology (the MIIT), the Ministry of Public Security (the MPS), and the State Administration for Market Supervision (the SAMR) jointly issued a ministerial regulation specifically for

[191] The Consumer Protection Law, Art 29 (2).
[192] Ibid, Art 29 (3).
[193] See representative cases where infringements on consumers' personal information were solved via consumer associations' mediation at: http://hjxt.cca.cn/cases/234.jhtml.
[194] For instance, the Consumer Association in Jiangsu Province launched a high-profile class action in 2018 against Baidu Apps' illegal collection and use of personal information. It is China's first representative suit on personal information protection. After Nanjing Intermediate Court accepted the case, Baidu quickly contacted the CCA and rectified its Apps following the Consumer Association's suggestions. The Consumer Association then withdrew the lawsuit. (See related news report at: https://www.thepaper.cn/newsDetail_forward_2028107). More recently, in September 2021, the Consumer Association in Chongqin City initiated a representative suit against a media company that disclosed the personal information of over 10,000 consumers who had purchased imported seafood later being found Covid-positive. The disclosed information includes name, address, national ID and so forth. The case was then settled via a mediation agreement before the court. (See news report http://www.cq.gov.cn/ywdt/jrzq/202109/t20210905_9659800.html, and https://www.pkulaw.com/news/42846a3981161324bdfb.html).
[195] See the full text of the Algorithm Provisions: http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm. A non-official English translation is available at https://www.chinalawtranslate.com/en/algorithms/.

regulating internet firms' use of algorithmic recommendation technology, entitled 'Provisions on the Management of Algorithmic Recommendation in Internet Information Service' (hereafter, the Algorithm Provisions). The Algorithm Provisions will take effect from 1st March 2022. While allegedly based on the PIPL, the DSL, and the CSL, the Algorithm Provisions seem to have moved beyond the established national laws and regulations, stipulating a wide range of rules for algorithmic recommendations, including (but not exclusive to) personalised advertising.[196]

For example, Art 24 of the Algorithm Provisions require providers of algorithmic recommendation services with public opinion properties or having social mobilization capabilities to report the provider's name, forms of service, the domain of application, algorithm type, algorithm self-assessment report and content intended to be publicised etc. through the internet information service algorithm filing system,[197] carrying out filing within 10 working days of providing services.

Likewise, the Algorithm Provisions impose a legal obligation on providers of algorithmic recommendation services to respect social mores and ethics, commercial and professional ethics, as well as follow the principles of justice, fairness, openness, and transparency, being rational and reasonable, and honest (Art 4). More specifically, algorithmic recommendation service providers are required, among others, to regularly review and assess their algorithm mechanisms, models, data, and outcomes, and thereby ensure that their algorithmic models will not induce users to become addicted, consume excessively, or to behave in a way that against laws, regulations, and social ethics. (Art 8). The Algorithm Provisions also prohibit the use of unlawful or negative information as users' interests or labels (Art 10). Price discrimination or other discriminating treatments alike are expressly banned (Art 21). Furthermore, the Algorithm Provisions particularly emphasises algorithmic recommendation service providers' obligation to protect minors online. This includes the requirements of developing user modes that suit minors, facilitate minors to obtain beneficiary and healthy information, and avoid recommending contents that may adversely affect minors' psychical and psychological health (Art 18).

What is more, the Algorithm Provisions further expand the rights of individual users in algorithmic recommendations. In addition to the right to opt-out personalised recommendations that had already been included in the PIPL and other national laws, the Algorithm Provisions grant individuals the right to select or delete user tags used by algorithmic recommendation service providers to target them (Art 17 (2)). In the case where the algorithmic recommendation has a significant impact on the rights and interests of individuals, the individual users also have the right to request an explanation from the service provider and to hold them liable. (Art 17 (3)). Another prominent feature of Algorithm Provisions is the 'categorised and graded administration system': according to Art 23, the regulators

[196] The applicable scope is defined in Art 2.

[197] The Internet Information Service Algorithm Filing System （互联网信息服务算法备案系统） was launched on 1 March 2022. See official notice about the launch of the system: http://www.cac.gov.cn/2022-02/25/c_1647395666889023.htm. The website of the system is: https://beian.cac.gov.cn.

will categorise and grade algorithmic recommendation service providers based on their capability of social influence, content categories, the scale of users, the degree of interfere in users' behaviours, the degree of sensitivity of data they handle etc. and thereby implement administration differently.

2. Provisions on the Cyber Protection of Children's Personal Information （《儿童个人信息网络保护规定》）[198]

The 'Provisions on the Cyber Protection of Children's Personal Information' is a ministerial regulation issued by the Cyberspace Administration of China (the CAC) in August 2019 specifically for the protection of personal information of children under the age of 14.[199] Before the enactment of the PIPL, the Provisions have played a critical role in regulating internet companies' collection and use of children's personal information. The PIPL now regards children's personal information as a special category of personal information that requires enhanced protection (Art 28); a few other rules are also included in the PIPL for the protection of children's personal information (Art 31). Nevertheless, the Children's Personal Information Protection Provisions will continue to be relevant, especially in the areas where the related rules are absent in the PIPL.

3. Interim Measures for the Administration of Internet Advertisements (《互联网广告管理暂行办法》) [200]

In July 2016, the State Administration for Industry and Commerce (the SAIC) issued the 'Interim Measures for the Administration of Internet Advertisements' (hereafter, the Interim Measures). The Interim Measures took effect from 1 st September 2016 and supplement the Advertising Law mentioned above.

The Interim Measures apply to all direct or indirect commercial advertising made through 'websites, webpages, software applications and other internet media' in various forms like text, image, audio, and video for advertising purposes, email solicitations, paid searches, and so forth (Art 3). The Interim Measures require internet advertisements, including paid search results, to be marked and easily identifiable as advertisements (Art 7). Internet advertising must not affect users' normal use of the internet; pop-up advertisements must provide an obvious close button and allow one-click close (Art 8 (1)). It is prohibited under the Interim Measures to include advertisements or links to advertisements in emails sent to users without their permission (Art 8 (3)). The Interim Measures also define the roles

[198] The full text of the Children's Personal Information Protection Provisions can be found at http://www.cac.gov.cn/2019-08/23/c_1124913903.htm. A non-official English translation is available at https://www.chinalawtranslate.com/en/childrenspersonalinfoonline/.
[199] Ibid, Art 2.
[200] The full text of the Interim Measures can be found at http://www.cac.gov.cn/2016-07/08/c_1119187555.htm. An non-official English translation is available at https://content.next.westlaw.com/0-521-4977?__lrTS=20210304152509438&transitionType=Default&contextData=%28sc.Default%29.

and responsibilities of different players in the internet advertising industry, such as advertisers, internet advertising operators, publishers, and a variety of intermediaries (Arts 9-15). [201]

Part III. National Standards & Self-regulation Guidelines

In addition to the national laws and regulations mentioned above, there are an increasing number of national standards and industry self-regulation guidelines in the Chinese legal system concerning personal information protection and/or online advertising.

Most notably, in March 2020, the Standardization Administration of China (SAC) and State Administration for Market Regulation (SAMR) jointly released the 'Information security technology—Personal information security specification' (GB/T 35273—2020)(《信息安全技术-个人信息安全规范》GB/T 35273—2020).[202] The Specification 2020 includes a comprehensive set of rules on personal information collection, storage, use, share, and disclosure, providing good practise guidelines for notice and consent, profiling, personalised recommendation, automated decision-making, and how to respond to individuals' requests to exercise their rights, etc. The release of Specification 2020 has gained great attention and received positive feedback worldwide.[203]

Many rules in the Specification 2020 are relevant for AdTech companies and their online advertising business. For instance, S5.3 requires data controllers to ensure individuals' freedom of choice in the phase of data collection, including not to request individuals to give bundled consent for multiple services/products/functions; not to use default consent but to require positive opt-in; not to frequently request consent or reduce the quality of service after the individuals have declined or exited from a particular function; not to coerce users to authorize data collection that is merely needed for increasing service quality, improving user experience, developing new products or enhancing security. Likewise, S 7.4 imposes a couple of restrictions on the use of user profiling: the characteristic description of individuals must not contain any pornographic, gamble-related, superstitious, horrific, or violent contents; must not contain contents that discriminate users based on their nations, ethnic groups, religions, disabilities, and diseases. According to S 7.5, where the personalised recommendation is used, the data controller must clearly differentiate personalised contents from non-personalised ones; they must establish a mechanism to facilitate users to exert independent control over the personal information on which the personal recommendations depend

[201] Noteworthy, on 26 November 2021, the State Administration for Market Regulation (i.e., a new ministry established in 2018 that consolidated several agencies including the State Administration for Industry and Commerce) released a draft 'Measures for the Administration of Internet Advertisements' for public consultation. The draft Measures, once adopted, will replace the current Interim Measures 2016. See https://www.samr.gov.cn/hd/zjdc/202111/t20211126_337380.html.
[202] The Specification 2020 is available in both Chinese and English at: https://www.tc260.org.cn/piss/js1.htm. The Specification 2020 took effect from 1 Oct 2020 and replaced its predecessor the 'Information security technology—Personal information security specification' (GB/T 35273-2017). The full text of the Specification 2017 can be found at: https://www.tc260.org.cn/front/postDetail.html?id=20180124211617.
[203] For example, see https://www.iflr.com/article/b1lt3cpmrmrd89/primer-chinas-new-personal-information-security-specification, and https://www.sia-partners.com/en/news-and-publications/from-our-experts/china-enters-new-era-data-protection-and-privacy.

(e.g., user labels and dimensions of profiling) and to adjust and control the degree of relevance of personalised recommendation.

Apart from the comprehensive Specification 2020, several other national standards have been drafted or/and adopted to address specific issues of personal information protection. These include, most notably, a guideline regarding the necessary information for mobile apps, [204] a guideline regarding the de-identification of personal information,[205] a guideline for personal information security impact assessment, [206] and a draft guideline on notices and consent. [207] Given the fact that the data protection rules in the PIPL are generally abstract and vague, these national standards and guidelines may provide great guidance for companies' data protection compliance work. Nevertheless, these guidelines are, by nature, voluntary and not legally binding. This means no direct penalty applies for contravention of the specifications per se, and supervisory authorities cannot use the guidelines as a direct legal basis for law enforcement. But the practical impact of the specifications might increase if administrative regulators and courts routinely refer to them in interpreting the rules in the PIPL and other national laws and regulations.[208]

Regarding industry self-regulation guidelines, China Advertising Association （the CAA） issued the 'Industrial Standard Framework of China Internet Targeted Advertisement Customer Information Protection[209] in 2014, and the 'Specification for Mobile Internet Advertising Identification' [210] and 'China Internet Advertising Delivery Monitoring and Verification Requirements' [211] in 2020. More recently, the Cyber Security Association of China (CSAC) released two draft guidelines for public comments in November 2021, namely, 'Guidelines for the Protection of Personal Information of Mobile Smart Terminals'[212] and 'Specifications for App Stores' Assessment and Management of

[204] 'Cyber security practice guide— Specification on essential information necessary for basic business functions of mobile Internet applications'（《网络安全实践指南—移动互联网应用基本业务功能必要信息规范》TC260-PG-20191A）, available at: https://www.tc260.org.cn/front/postDetail.html?id=20190531230315.

[205] 'Information security technology—Guide for de-identifying personal information （《信息安全技术 个人信息去标识化指南》GB/T 37964-2019）', available at: http://std.samr.gov.cn/gb/search/gbDetailed?id=91890A0DA4AB80C6E05397BE0A0A065D.

[206] 'Information security technology—Guidance for personal information security impact assessment (《信息安全技术 个人信息安全影响评估指南》GB/T 39335-2020)' , available at: http://std.samr.gov.cn/gb/search/gbDetailed?id=B4C25880C3DE1CB3E05397BE0A0A92D0.

[207] 'Information security technology -Guidelines for personal information notices and consent (draft for public consultation)（《信息安全技术个人信息告知同意指南(征求意见稿)》）' available at: http://std.samr.gov.cn/gb/search/gbDetailed?id=C1A8A075C122B46EE05397BE0A0A6991.

[208] See: 许可：'《个人信息安全规范》的效力与功能'， 数字经济与社会，25 April 2019 https://www.secrss.com/articles/10176.

[209] Its Chinese title is 《中国互联网定向广告用户信息保护行业框架标准》and the full text is available at: http://www.lawinfochina.com/display.aspx?id=20938&lib=law.

[210] Its Chinese title is: 《互联网广告标识技术规范（T/CAAAD 003-2020）》and the full text is available at: http://www.china-caa.org/uploads/downloads/caidguifan.pdf.

[211] Its Chinese title is: 《中国互联网广告投放监测及验证要求 (T/CAAAD 002—2020)》and the full text is available at: http://www.china-caa.org/uploads/downloads/digital/ggtfjcjyzyq.pdf.

[212] Its Chinese title is: 《 移动智能终端个人信息保护指南 (征求意见稿) 》, and the full text is available at: https://www.cybersac.cn/News/getNewsDetail/type/64/id/1891.

Personal Information Collection and Use by Apps'. [213] The two documents respectively focus on the personal information protection responsibilities of mobile device manufacturers and app stores, However, the non-binding nature of the guidelines together with the absence of enforcement mechanism means that the practical impact of these industry self-regulation guidelines is likely to be very limited.

[213] Its Chinese title is: 《应用商店 App 个人信息收集使用上架审核和管理规范（征求意见稿）》and the full text is available at: https://www.cybersac.cn/News/getNewsDetail/type/64/id/1891.

Annex Three

China - Special Rectification Scheme for Mobile Apps (2019 – 2022)

Dr. Li Yang
Research Associate / 博士后研究员
King's College London

Part 1. Introduction

In January 2019, four ministries of the Chinese central government, namely, the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), the Ministry of Public Security (MPS), and the State Administration for Market Supervision (SAMR), jointly launched 'Special Rectification Scheme on Illegal Collection and Use of Personal Information by Apps'. [214] This Special Rectification Scheme is China's most intensive, well-known, and long-lasting data protection enforcement in the AdTech industry by far. By November 2021, the Special Rectification Scheme has issued rectification notices to over 5,400 mobile apps, publicly named about 2050 apps that failed to rectify their personal information processing practices following the regulators' notices, and removed 540 apps from app stores.[215] Many mobile apps developed by top Chinese AdTech Companies, including Tencent, Alibaba, Baidu, Douyin (i.e., Chinese Tiktok), Xiaomi, Didi, etc. were among those being publicly named or/and removed from app stores.[216]

Initially, the Special Rectification Scheme on Apps was planned to operate for only one year and was supposed to end in December 2019, according to the official announcement issued in January 2019.[217] In reality, however, the Special Rectification Scheme has continued into the years 2020 and 2021. Furthermore, in April 2021, the MIIT released a draft ministerial regulation for public comments[218], which states that the CAC, the MIIT, the MPS, and the SAMR are to establish a 'collaborative supervisory and administrative work mechanism on the protection of personal

[214] 'Announcement on Launching a Special Rectification Scheme on the Illegal Collection and Use of Personal Information by Apps' (《关于开展 App 违法违规收集使用个人信息专项治理的公告》), 23 January 2019 http://www.cac.gov.cn/2019-05/23/c_1124532020.htm.
[215] White Paper on Personal Information Protection Governance in Mobile Internet Application (APP)' (《移动互联网应用程序(app)个人信息保护治理白皮书》), November 2021 http://www.caict.ac.cn/kxyj/qwfb/bps/202111/P020211119513519660276.pdf, at p 16.
[216] The Chinese regulators' enforcement notices can be found at: https://www.miit.gov.cn/jgsj/xgj/APPqhyhqyzxzzxd/tzgg/index.html.
[217] See the Announcement above.
[218] 'Interim Provisions on the Protection and Management of Personal Information in Mobile Internet Apps (Draft for Solicitation of Comments)') (《移动互联网应用程序个人信息保护管理暂行规定(征求意见稿》)), 26 April 2021 http://www.cac.gov.cn/2021-04/26/c_1621018189707703.htm.

information in apps'.[219] In other words, the joint data protection enforcement scheme on apps probably will likely be the norm in near future.

Different from the EU and the UK, the Chinese regulators have directed most of their attention to the personal information protection in the mobile advertising ecosystem, in particular mobile apps. This is probably because the large majority of China's online advertising is mobile advertising which relies principally on mobile apps rather than web browser cookies. According to a 2020 report on the Chinese AdTech industry, between the year 2018 and the year 2021, mobile advertising has persistently accounted for over 88% of China's online advertising market, whereas 'PC advertising' (i.e., personal computer-based advertising) accounts for only 10.8 % in 2018 and projects to account for only 5.6 % in 2021 and 4.6% in 2022. [220] This distinction in regulatory focus means that the Chinese experiences on regulating mobile apps may nicely complement the current discussions in the EU and the UK that focus primarily on web browser cookies.

Specifically, some lessons that have been learned by the Chinese regulators while carrying out the Special Rectification Scheme. These lessons and experiences accumulated through years of intensive regulatory practices, we believe, might be worth noticing and considering for experts here in the EU and the UK.

To start with, the Chinese regulators have found that whilst most mobile apps, on the surface, had obtained the users' consent in accordance with the laws and regulations, there are many problems in the ways that the notice and consent are conducted in practice.[221] In other words, the Chinese regulators have recognised the prevailing problem of 'dark patterns'[222] in the mobile app environment and the Chinese AdTech industry, although the term is not used.

For example, when notifying the users, some apps provide privacy policies that are difficult to read for users (e.g., the text is overly small or dense, the colour is too light, fuzzy, or only traditional Chinese version is provided), or difficult to access (e.g., after entering the main interface of the app, it takes numerous clicks to access the text). Some apps do not use a pop-up window or other obvious means to remind users to read the privacy policy.[223] It is also commonplace for apps to request consent for the collection of personal information that is unnecessary for the service or unreasonable for the contexts, such as the excessive collection of users' contacts, location, citizen ID numbers, and facial information. There are also coercive notice and consent in varied forms. Apart from the most obvious form of 'no consent, no access', some apps frequently and repeatedly ask for the users' consent, even though the users had explicitly rejected such request, whereas some others sneakily collect information beyond the scope of authorised by the users. There are also cases where apps, after the

[219] Ibid, Art 4.
[220] See: https://www.questmobile.com.cn/research/report-new/151.
[221] See details in the diagram below.
[222] See discussions about the dark patterns in Section 7 of the main report.
[223] See details in the diagram below.

user expressly declined the information collection request, continue to collect personal information, or change the permission set by users without the user's consent (e.g., automatically reset the permissions to the default state when the app is updated). [224]

There are also man-made obstacles for users to exercise the data subject rights expressly granted by laws and regulations. Many apps, for instance, do not provide the users with the information about their data subject rights, or/and the ways to exercise such rights (e.g., no option is provided for users to opt-out personalised recommendations and advertisements; no way to cancel a user account). It is also not uncommon for apps to set up excessively burdensome procedures and unreasonable conditions for users to exercise their data subject rights. [225]

Secondly, the Chinese regulators have recognised, based on their enforcement experience, that compliance in paper or privacy policy does not necessarily mean compliance in practice. Technical examination and monitoring, therefore, are essential for ensuring genuine data protection compliance and effective data protection enforcement.

In a report issued by the Chinese regulators in the mid-2020 based on their Special Rectification work in 2019,[226] it is noted that 'Some apps use encrypted data packets when excessively collecting personal information, some apps can identify the test environment and prevent inspection tools from detecting their abnormal transmission behaviours, whereas some apps bypass the mobile device operating system permission control mechanism and obtain users' the Unique Identifier of the Device by reading the external storage area.' [227] Moreover, rapid updates of apps (this means that the status of compliance or non-compliance can change swiftly) and the enormous number of new apps entering the market make the data protection regulation even more challenging. [228] Without concrete technical support, as the report stressed, the efficacy of data protection supervision and enforcement would be significantly undermined.[229]

For this reason, the Chinese regulators have begun to establish the 'National Technology Testing Platform for App' (全国 APP 技术检测平台) [230]since 2020. The Testing Platform not only provides technical support for local regulatory authorities to conduct data protection inspection on apps but also offers an accessible way for app developers and operators to self-check their apps and thereby

[224] Ibid.
[225] Ibid.
[226] 'APP Special Governance Report on the Collection and Use of Personal Information in Violations of Laws and Regulations (2019)'《APP 违法违规收集使用个人信息专项治理报告（2019）》, released in May 2020, http://www.cac.gov.cn/2020-05/26/c_1592036763304447.htm.
[227] Ibid, at p 24.
[228] Ibid.
[229] Ibid.
[230] The official website of the testing platform is: https://app.caict.ac.cn/#/home.

ensure data protection compliance. [231] According to the statistics from the Ministry of Industry and Information Technology (MIIT), 2.08 million mobile apps were tested in the year 2021 alone.[232]

Thirdly, the regulators have also realised in the course of their enforcement practices that 'app personal information protection issues are not only related to apps per se, but also mobile device manufacturers (e.g., smartphone manufacturers), app distribution platforms (e.g., app stores), and third parties (e.g., third-party SDKs and partners)'.[233] In other words, 'It is a complex mobile ecological issue' that the regulators are facing and tackling. [234]

Most notably, the use of third-party SDKs has become an important part of the mobile ecosystem. The software development kit (SDK) is commonly embedded during the process of app developments to help quickly obtain the functions of advertising, payment, statistics, information push, social networks, maps, positioning etc. provided by third parties. While the SDK greatly improves development efficiency and reduces costs for app developers, the security of the SDK itself and its collection and use of personal information have also become a high-risk point for personal information protection in the mobile ecosystem.[235] What is more, apps must run on a mobile device, whereas apps' design concept , grouping and grading of permissions, and permission application mechanism are all subject to the mobile device's operating system. Considering that Android, the dominant mobile operating system in the Chinese market, allows mobile device manufacturers to develop and optimize the system based on its open-source project, it is important to ensure the mobile device manufacturers are compliant with laws, regulations and national standards and implement privacy-friendly design concept when optimising the Android system. [236] In addition, apps usually need to go through an online assessment of the app distribution platforms (i.e., app stores) before becoming available for users. However, there were not yet unified requirements and criteria for apps' information protection and security assessment by app distributors in China.[237] Consequently, the Chinese regulators have been gradually expanding their regulatory targets from the app operators and developers, to also include app distribution platforms and third-party SDK providers. [238]

---

[231] See ' White Paper on Personal Information Protection Governance in Mobile Internet Application (APP)' (《移动互联网应用程序(app)个人信息保护治理白皮书》), November 2021 http://www.caict.ac.cn/kxyj/qwfb/bps/202111/P020211119513519660276.pdf, at pp 11-12.

[232] See: https://news.cctv.com/2022/02/28/ARTIbkjsSRaF1JN0Hqgl48yv220228.shtml.

[233] See 'APP Special Governance Report on the Collection and Use of Personal Information in Violations of Laws and Regulations (2019)'《APP 违法违规收集使用个人信息专项治理报告（2019）》, released in May 2020, http://www.cac.gov.cn/2020-05/26/c_1592036763304447.htm, at pp 22-23.

[234] Ibid.

[235] Ibid. According to a 2020 report on the security and legal compliance of the SDK published by the CAICT, an affiliate research institute of the MIIT, on average one mainstream app in the market contains about 10 SDKs. For certain categories of apps, the average number of third-party SDKs can be over 30. Moreover, the SDK developers tend to 'expand the functions of their SDKs horizontally and vertically', thereby increasing the SDKs' ability in accessing and combining data from different variety of apps and business contexts. It is also indicated in the report that personal information collection and use by the SDK is not only beyond the awareness of ordinary individual users, but also sometimes can be a 'black box' for the app developers. See: http://www.caict.ac.cn/kxyj/qwfb/ztbg/202009/P020200928658526802640.pdf, pp13-14 and 19-21.

[236] See the White Paper above, at p 23.

[237] Ibid.

[238] See details about the chronological evolution of the Special Rectification Scheme in the Diagram below. Also,

Admittedly, the impact of these Special Rectification Scheme on Apps is not yet satisfying. Despite the regulators' active and intense enforcement activities since 2019, there are still a considerable number of apps in the markets that collect and use personal information in ways against the laws and regulations, including some apps developed by the top Chinese AdTech companies. [239] The major reason is that the legal consequences for the non-compliant apps—i.e., ordering to correct and public naming in most cases, are far from deterring. Only those apps that refuse rectification or fail to pass the re-evaluation might be asked by the regulators to be temporarily removed from app stores. The newly enacted Personal Information Protection Law (the PIPL) gives the supervisory authorities the power to impose an administrative fine of up to 50 million RMB or 5 per cent of annual turnover.[240] If adopted in the enforcement against apps that illegally collect and use personal information, it may significantly increase the effectiveness of the Special Rectification Scheme.

Part 2. Chronological evolution of the Special Rectification Scheme

The diagram below aims to offer an accessible overview of the chronological evolution of the ongoing Special Rectification Scheme for Mobile Apps in China. The diagram lists the major policies and reports issued by the Chinese regulators under the Special Rectification Scheme since its start in January 2019. The main contents of the documents are also summarised and included in the diagram.

Document No. (by issue date)	**Title, Date & Authority**	**Main Contents**
No 1.	'Announcement on Launching a Special Rectification Scheme on the Illegal Collection and Use of Personal Information by Apps' (《关于开展 App 违法违规收集使用个人信息专项治理的公告》) Issued on 23 Jan 2019 by four ministers, namely, the CAC, the MIIT, the MPS, and the SAMR. Available at: http://www.cac.gov.cn/2019-05/23/c_1124532020.htm.	It is announced that the four ministries jointly launch a special rectification scheme on the illegal collection and use of personal information (hereafter, PI) by mobile apps which will last from January to December 2019. The Special Rectification Scheme consists of five main aspects: First, to ensure that app operators strictly fulfil the obligations imposed by the Cybersecurity Law, adopt effective information security measures, observe the principles of lawfulness, legitimacy, and necessity, observe the rule of transparency and informed consent, and not to use PI in ways against, laws, regulations and the agreement with users. App operators are also required to provide users with non-personalised options when pushing up targeted news and ads. Secondly, the Standardization Administration of China, Consumer Protection Association, and China Internet Association will make guidelines for commonly used

on 28 February 20222, the director of the MIIT stated in a press conference that in the year 2022, they will deepen the regulation of apps, aiming to cover all type of terminals (phones and tablets etc.) and all responsible parties and phases, in particular, the app stores, third-party SDKs and the pre-installation phase. See the related news report at:
https://news.cctv.com/2022/02/28/ARTIbkjsSRaF1JN0Hqgl48yv220228.shtml.

[239] See the Chinese regulators' recent enforcement activities: https://www.miit.gov.cn/jgsj/xgj/APPqhyhqyzxzzxd/tzgg/index.html.

[240] See more details about the PIPL in Annex 2.

		apps regarding their essential functions and necessary information and assessment criteria for apps' PI governance, and organise specialised institutions to assess the privacy policies and PI processing activities of the apps with a large number of users. Thirdly, it calls local authorities to actively enforce data protection rules in the Cybersecurity Law and the Consumer Protection Law. Fourthly, it states that public security organs (i.e., Chinese police) will strengthen their work in combating PI-related crimes. At last, it also announces the launch of the 'APP PI Security Certification Scheme', encouraging app operators to join in the Certification scheme and asking app stores and search engines to clearly mark and prioritize the certificated apps in their recommendations.
No 2.	'Announcement on Carrying out the Work of App Security Certification'(《关于开展 App 安全认证工作的公告》), and its attachment, 'Implementation Rules for Safety Certification of Mobile Internet Application (app)'(《移动互联网应用程序（App）安全认证实施规则》) Issued on 13 March 2019 by the CAC and the SAMR. Available at: http://www.cac.gov.cn/2019-03/15/c_1124240900.htm.	Following the initiation of the Special Rectification Scheme in January, the CAC and the SAMR announced the start of Certification work from March 2019 and released the 'Implementation Rules for Safety Certification of Mobile Internet Application'. The 'Implementation Rules' specify the applicable scope of the App Security Certification, and the certification criteria, procedure and time frame of the certification process, as well as certification bodies' responsibility in technically testing the app, on-site auditing the app operators, and monitoring the apps after certification is granted. It also specifies the correct ways for certificated apps to use the certification mark. The App Security Certification, however, is not compulsory. Instead, the authorities merely encourage apps to voluntarily join in the Certification Scheme by asking search engines and app stores to prioritize certificated apps in their recommendation and to display the certification mark. By October 2021, there are only 24 apps of 14 app operators being granted the Security Certification.[241] This is a rather marginal number, given the fact that there are over 2.7 million mobile apps in the Chinese market.[242] Unless the Certification becomes a mandatory condition for apps to be offered in app stores, the pragmatic impact of the Security Certification is likely to be limited.
No 3.	'Notice of the Ministry of Industry and Information Technology on Launching Special Rectification Work	According to the Notice, both app operators and app distribution service providers (i.e., app stores) will be the regulatory targets. The Notice also sets three main phases for the Special Rectification Scheme. **Phase I**

[241] See related news report: http://it.people.com.cn/n1/2021/1014/c433780-32253530.html.
[242] See: http://www.workercn.cn/34196/202111/02/211102101516011.shtml.

	for APP Infringing on the Rights and Interests of Users'(《工业和信息化部关于开展 APP 侵害用户权益专项整治工作的通知》) Issued on 31 Oct 2019 by the MIIT. Available at: http://www.gov.cn/fuwu/2019-11/07/content_5449660.htm	(from 31 Oct to 10 Nov 2019): enterprises' self-check and rectification; **Phase II** (11 Nov to 30 Nov 2019): supervision and random inspection by the telecommunication administration authorities, including assigning third-party testing institutions to conduct technical inspecting on apps and organising China Internet Association, and related experts and media to evaluate apps that are widely complaint by the public; **Phases III** (1 Dec to 20 Dec 2019): imposing penalties according to the inspect results, such as ordering to rectify, public naming, removing the apps from app stores, cutting off the connection of the apps, and including the non-compliant entities into the list of untrustworthy or bad business operators. The Notice also indicates four categories and eight data protection issues that the authorities will focus on in carrying out the Special Rectification Scheme: Category 1: Collecting users' PI in violation of laws and regulations. (1) collecting PI without first informing the users of the purpose, method, and scope of the PI use and obtaining the consent from the users; (2) excessive PI collection, i.e., the apps collect PI unnecessary for the services or unreasonable for the contexts, or excessively and over-frequently collect PI, such as contacts, location, citizens' ID numbers, and facial information. Category 2: Using users' PI in violation of laws and regulations. (3) sharing PI with other apps without the users' consent, such as device identification information, browsing records, search habits, commonly-used software app lists, etc. (4) the apps force users to use the targeted push function. That is, the apps do not inform the user of the facts about the targeted recommendations and advertisements or do not provide options for users to turn off the personalised function. Category 3: The unreasonable request of users' permissions/consents. (5) 'no permission/consent, no use/access.' That is in the process of installation, the app asks users for permissions that have nothing to do with the current service scenario; or when the users decline, the app exits or closes. (6) 'overly frequent requests for permission'. That is after the users explicitly reject the permission request, the app still frequently and repeatedly asks for permissions that are not related to the current service scenario. (7) 'excessive request of permissions.' That is, even when the users do not use the related functions or services, the app still asks for permissions to open the contacts, location, text message, recording, camera, etc. in advance, or request permissions beyond what is necessary for the services or functions. Category 4: Setting up obstacles for users to cancel the account. (8) the app fails to provide users with account cancellation services or sets up unreasonable obstacles for the cancellation.

No 4.	'Measures for the Determination of the Collection and Use of Personal Information by Apps in Violation of Laws and Regulations' (《App 违法违规收集使用个人信息行为认定方法》) Issued on 28 Nov 2019 by the CAC, the MIIT, the MPS and the SAMR. Available at: http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm.	The document specifies the situations or acts that will be considered as violating the laws and regulations under the Special Rectification Scheme on Apps. 1. The following behaviours will be considered as 'failing to disclose the information collection and use rules', including (1) no privacy policy is provided in the apps, or there is no rule for the collection and use of PI in the privacy policy; (2) when the apps operate in the first time, there is no pop-up window or other obvious means to remind users to read the privacy policy; (3) the privacy policy is difficult to access (e.g. after entering the main interface of the apps, it takes more than 4 clicks to access); (4) the privacy policy is difficult to read (e.g., the text is too small or dense, the colour is too light, fuzzy, or the simplified Chinese version is not provided). 2. The following behaviours will be considered as 'failure to clearly state the purpose, method, and scope of the PI collection and use': (1) the purpose, method, and scope of PI collection and use (including the entrusted third parties or embedded third-party codes, plug-ins, etc.), are not listed one by one; (2) when the purpose, method, or scope of the PI collection and use change, the users are not notified of the changes in proper manners. (3) when asking for permissions to collect PI, or when collecting sensitive PI (such as citizens' ID numbers, bank account, etc), the users are not informed of the purpose simultaneously, or the notice is unclear and difficult to understand; (4)the contents of the PI collection and use rules are obscure, excessively long and cumbersome, and difficult for users to understand (e.g., use a large number of professional terms). 3. The following behaviours will be regarded as 'collecting and using PI without the users' consent': (1) collecting PI or turning on the permission to collect PI before obtaining the user's consent; (2) after the users expressly decline, the app still collects PI or open the permission to collect PI, or frequently/repeatedly ask for the users' consent/permission; (3) the actual collected PI or the opened permissions by the app exceed the scope of users' authorization; (4) soliciting users' consent in non-explicit ways, such as default consent; (5) change the PI collection permission set by users without the users' consent (e.g., automatically reset the permissions to the default state when the app is updated); (6) using algorithms and PI to push up targeted/personalised information without providing the users the alternative options; (7) misleading users to give consent or turning on permissions to collect PI via fraud, deception, or other improper methods (e.g., deliberately deceiving or concealing the true purpose of PI collection); (8) failure to provide users with the means to withdraw consent; (9) collecting and using PI in a way that violates the stated collection and use rules.

		4. The following behaviours will be regarded as 'violating the principle of necessity and collecting PI irrelevant to the services provided': (1) the type of PI collected or the permission to collect PI opened have nothing to do with the existing business functions;(2) refusing to provide services/products/functions because the users do not consent to the collection of the unnecessary PI or to open the unnecessary permissions;(3) the PI collected by the app's new functions exceeds the scope of the users' original consent, and if the users refuse to give new consent, the original business function stops working. The exemption applies where the new business function replaces the original function; (4) the frequency of PI collection exceeds the actual needs of functions; (5) forcing users to consent to the PI collection solely on the grounds of improving service quality, enhancing users' experience, pushing targeted information, developing new products, etc.; (6) requiring users to give a bundled consent, or to open multiple permissions at one time, and if the users decline, the app cannot be used. 5. The following behaviours will be considered as 'providing PI to others without consent' : (1) without the users' consent or anonymization, the app provides PI to a third party, including PI provision through third-party codes, plug-in etc. embedded in the client-side server; (2) without the users' consent or anonymization, providing PI to a third party after the PI is transmitted to the app's backend server; (3) the app connects to a third-party app without the user's consent and thereby provides PI to the third-party app. 6. The following behaviours will be regarded as 'failure to provide the function of PI deletion and rectification according to the laws and regulations' or 'failure to publicising information regarding complain and report methods.' : (1) failing to provide valid functions for PI rectification, deletion, and account cancellation t;(2) setting up unnecessary or unreasonable conditions for PI rectification, deletion, or account cancellation; (3) although the related functions are provided, the app operator fails to respond to the users' requests promptly; and where manual processing is needed, the app fails to respond within the committed time frame (the committed time limit shall not exceed 15 working days).
No 5.	'APP Special Governance Report on the Collection and Use of Personal Information in Violations of Laws and Regulations (2019)' (《APP 违法违规收集使用个人信息专项治理报告（2019）》)	The Report explains the social and legal backgrounds of the launch of the Specifical Rectification Scheme for Apps, as well as the major works conducted by the four ministries under the Scheme in the year 2019. According to the Report, five major works have been conducted under the Specifical Rectification Scheme: firstly, several complain and report channels are established which enable consumers to conveniently report apps that misuse their PI. For example, the 'APP PI Reporting (App 个人信息举报)' is a reporting channel

	Released in May 2020 by the Personal Information Protection Task Force on Apps (APP 专项治理工作组), a special task force jointly established by the four ministries under the Special Rectification Scheme.[243] Available at: http://www.cac.gov.cn/2020-05/26/c_1592036763304447.htm.	established on China's most popular social media, WeChat. It alone received 1,2125 reports/complaints concerning over 2300 apps by December 2019. [244] Secondly, several documents are issued to provide detailed guidance for app operators and local authorities regarding the criteria of illegal collection and use of PI. Thirdly, the authorities have selected and commissioned 14 professional testing agencies to assess apps' PI collection and use. Fourthly, the authorities have launched the APP PI Security Certification scheme, encouraging apps to voluntarily join in the Certification and thereby increasing their PI protection level. [245] Lastly, thousands of mobile apps, including apps developed by large Chinese AdTech companies, were publicly named, or/and required to rectify their PI collection and use practices.[246] The Report also evaluated the effectiveness of the Special Rectification Scheme by comparing the statics about the apps in January 2019 and at the end of 2019 and via public surveys. The Report considers the impact of the Special Rectification Scheme as 'prominent'. But the statistics show that over 25% of apps in the sixth inspection at the end of 2019 failed to notify users of the purpose, method, and scope of their PI collection and use, whereas approximately 10 % of the apps provided PI to others without the users' consent. In the meantime, the Report also points out several new problems discovered by the authorities when carrying out the Special Rectification Scheme. In particular, they found that 'app's PI protection issues are not only related to apps per se but also mobile device manufacturers (e.g. Smartphone manufacturers), app distribution platforms (app stores), and third parties (third-party SDKs and partners). It is 'a complex mobile ecological issue', the report stressed. It is also noted in the Report that the Special Rectification has moved from detecting and handling typical data protection problems into the 'deep-water areas' where problem identification, evaluation, and judgment all require further research. The support from technology experts is particularly crucial for the work.
No 6.	'Notice of the Ministry of Industry and Information Technology on Carrying on and Deepening the Special Rectification Action on Apps Infringing Users' Rights and Interests' (《工	The Notice announces that the regulators are to continue with and deepen the Special Rectification Scheme for Apps, and the new wave of actions will start from 28 July 2020 and end on 10 Dec 2020. According to the Notice, the regulatory targets of the new enforcement actions are expanded to include SDK

[243] The official website of the Personal Information Protection Task Force on Apps is: https://pip.cybersac.cn/.
[244] Also see: https://pip.cybersac.cn/jbxt/privacy/index.
[245] See: https://www.isccc.gov.cn/zxyw/cprz/ydhlwrz/index.shtml.
[246] For example, see: http://www.gov.cn/xinwen/2021-05/15/content_5606714.htm； http://www.cac.gov.cn/2020-11/17/c_1607178245870454.htm； http://www.cac.gov.cn/2021-06/11/c_1624994586637626.htm；

	信部关于开展纵深推进 App 侵害用户权益专项整治行动的通知》) Issued on 28 July 2020 by the MIIT. Available at: http://www.gov.cn/zhengce/zhengceku/2020-08/02/content_5531975.htm.	providers and app distribution platforms (i.e., app stores). The Notice also announced that the 'National Technology Testing Platform for App' (全国 APP 技术检测平台) [247]was to be established by the end of August 2020; and the Testing Platform is aimed at testing 400, 000 mainstream apps in the Chinese market by 10 December 2020.
No. 7	'Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications' (《常见类型移动互联网应用程序必要个人信息范围规定》) Issued on 12 March 2021 by the CAC, the MIIT, the MPS and the SAMR. Available at: http://www.cac.gov.cn/2021-03/22/c_1617990997054277.htm.	The Provisions list and specify the 'necessary PI' for 39 types of common apps. For example, It is stated in the Provisions that for map and other navigation service apps, the basic function is 'positioning and navigation', and the necessary PI include location information, place of departure, and place of arrival; for car-hailing apps, the basic function is 'online taxi booking service and cruise taxi calling service', and the necessary PI includes the user's mobile phone number, the departure place, arrival place, location information, as well as payment information such as payment time, amount, and method.
No. 8	'Interim Provisions on the Protection and Management of Personal Information in Mobile Internet Apps (Draft for Solicitation of Comments)' (《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》) Released by the MIIT for public comments on 26 April 2021. Available at: http://www.cac.gov.cn/2021-04/26/c_1621018189707703.htm.	On April 2021, the MIIT released the draft Regulation for public comments (once enacted, the Provisions as ministerial regulation will have a higher authority level than other documents indicated above). According to the draft Provisions, the 'collaborative work mechanism' between the CAC, the MIIT, the MPS, and the SAMR is to be established' to supervise the protection of personal information by apps (art. 4). Relevant industry organizations and institutions will carry out APP PI Protection Ability Assessment and Certification in accordance with the laws and regulations. (art. 5) Noteworthy, the draft Provisions not only include data protection rules for app operators and developers, but also app distribution platforms (art. 9), apps' third-party service providers (art.10), mobile device manufacturers (art. 11), and network access providers (art.12).

[247] See: https://app.caict.ac.cn/#/home.

No. 9	'Notice of the Ministry of Industry and Information Technology on the Promotion of Awareness and Perception Regarding Information and Communication Services'(《工业和信息化部关于开展信息通信服务感知提升行动的通知》) Issued by the MIIT on 1st November 2021. Available at: http://www.gov.cn/zhengce/zhengceku/2021-11/06/content_5649420.htm.	The MIIT issued the Notice on 1st November 2021, the date the PIPL took effect, advocating local telecommunication administration authorities, telecommunication companies, and internet firms to improve the quality of their services, and thereby 'promote users' sense of security, gain, and happiness.' Among others, the Notice stipulates three requirements concerning apps' personal information protection: Firstly, internet companies are required to optimize the way their privacy policies and permission requests are displayed, and thereby ensure that the users are fully informed of the PI collection and use. Secondly, internet companies are required to optimize the display of pop-up windows, making sure that the close buttons are easy to identify, easy to click, and not misleading. Most notably, the Notice requires internet companies to create 'Dual Lists 双清单' (i.e., a list of the PI collected, and a list of the PI shared with third parties) and display them in the secondary menu of apps to facilitate users' inquiry.
No. 10	'White Paper on Personal Information Protection Governance in Mobile Internet Application (APP)' (《移动互联网应用程序(app)个人信息保护治理白皮书》) Issued in November 2021 by China Academy of Information and Communications Technology (the CAICT), an affiliate research institute of the MIIT. Available at: http://www.caict.ac.cn/kxyj/qwfb/bps/202111/P020211119513519660276.pdf.	The Report explains the rationales behind China's increasing regulation of apps' personal information protection and outlines the regulatory works conducted in the previous years and the vision for the future regulatory work. Specifically, the White Paper indicates four main areas that the Chinese regulators will focus on when deepening the regulation of apps' personal information protection: firstly, to strengthen and complete the legal basis for the regulation. It is noted in the White Paper that China's personal information protection regime has been established following the recent enactment of the Personal Information Protection Law and the Data Security Law. However, the national laws are mainly statements of principles and lack targeted rules for the regulation of apps, whereas internet apps represent a field full of technical innovations, dynamic changes, and new problems. The Chinese regulators, therefore, will adopt specialised regulations and industry standards for personal information protection by apps in near future. Secondly, to establish and improve the cooperation mechanism between different regulators and between central and local regulators, finding ways to gradually shift from addressing typical problems to comprehensive supervision and regulation. Thirdly, to make good use of technological tools in personal information protection supervision and enforcement. This, in turn, requires the establishment and optimization of the Technology Testing Platform as

		well as clear, fair and transparent testing rules and procedures. Lastly, to promote public education about personal information protection and encourage the participation of all related parties such as governments, enterprises, organisations, and individuals, thereby fostering a co-governance system for the protection of personal information in China.
No. 11	'Notice on Further Regulating the Pre-Installation Behaviour of Mobile Smart Terminal Application Software (Draft for Solicitation of Public Comments) (《关于进一步规范移动智能终端应用软件预置行为的通告（征求意见稿）》)' Released by the MIIT on 16 February 2022. Available at: https://www.miit.gov.cn/gzcy/yjzj/art/2022/art_e50ed15ce3a84adc849f5a8563d0a24f.html.	The Notice requires mobile device manufacturers to ensure that all pre-installed apps, except those for specified essential functions, can be uninstalled, and to provide users safe and convenient methods to uninstall. It also requires mobile device manufacturers to adopt appropriate technical to improve the security of operating systems, thereby preventing the replacement of operating systems or the installation of apps during product circulation/transmission.