Table of contents

1. Executive summary

The Office of the Australian Information Commissioner (OAIC) commissioned Information Integrity Solutions (IIS) to conduct a global scan of how other global jurisdictions have approached the regulation of data practices of digital platforms. The OAIC requested a descriptive research paper (without additional analysis and commentary) that examined regulators' actions and strategies in this area. The goal of this paper is to inform the OAIC's own thinking, position and strategy within its sphere of action.

1.1 Key observations

Digital platforms pose unique challenges for the privacy of users and for data protection authorities overseeing the enforcement of privacy law. These range from difficulties associated with their cross-border operation, to information asymmetries negatively impacting users, to the challenges of meaningful consent, to the complexity and extensiveness of adtech data processing. Many of these challenges also have the effect of diminishing the control individuals have over their personal information.

This paper identifies some of the ways that other jurisdictions are meeting these challenges. These include:

- **Expanding the extraterritorial operation of data protection law** to ensure platforms based in other jurisdictions but operating globally can be held to account.
- **Expanding the definition of personal information** to ensure that data involved in online tracking, profiling and targeted advertising is covered by the definition and therefore brought under the operation of data protection law.
- **Strengthening penalty provisions** in data protection law to enable imposition of fines that reflect the size and revenue of the tech giants and therefore better incentivise compliance.
- **Strengthening transparency requirements** (including mandatory breach reporting) and using enforcement powers to pursue platforms with deficient transparency measures in place or misleading privacy information.
- **Expanding individual rights** by legislating the right to erasure, the right to object and others and removing exceptions to these rights when it comes to profiling, advertising, sale of personal data and use of children’s data.
- **Giving enforcement attention to ‘lawful basis for processing’** in the context of targeted advertising and examining the adequacy of consent mechanisms.
- **Seeking evidence of good privacy governance** by mandating data protection by design and data protection impact assessments in some circumstances (particularly in relation to profiling activities).

Data protection authorities are particularly grappling with the privacy issues associated with targeted advertising and the difficulty of reconciling the data maximisation requirements of the adtech industry with the data minimisation principles of most privacy law.

2. Introduction

OAIC commissioned IIS to conduct a global scan of how other global jurisdictions have approached the regulation of data practices of digital platforms. The OAIC requested a descriptive research paper (without additional analysis and commentary) that examined regulators' actions and strategies in this area. The goal of this paper is to inform the OAIC's own thinking, position and strategy within its sphere of action.

In drafting this paper, IIS has maintained a focus on jurisdictions external to Australia. While there are relevant regulatory and reform activities occurring in Australia at present, these are not the focus of the paper. OAIC is already familiar with the Australian regulatory landscape in 2020 and has sought to expand its understanding of other approaches.

The paper is presented in two parts.

- Part A presents the research by theme. It outlines five key privacy challenges posed by the operations of digital platforms and summarises some of the ways other jurisdictions are meeting those challenges.
- Part B offers a description of regulatory approaches to digital platforms by jurisdiction. The focus of this research has been to provide a snapshot of the privacy regime in each respective jurisdiction and describe regulatory and enforcement activities focused on digital platforms.

2.1 Meaning of 'digital platforms'

This research paper focuses on **social media platforms** and **search engines**. In Australia, the top two digital platforms are Google (which includes YouTube, Gmail and so on) and Facebook (which includes WhatsApp, Instagram, Messenger and so on). Figures from 2019 show that Australians spend 20 percent of their time on Google and Google-owned services and 18 percent of their time on Facebook and Facebook owned services.[1] These represent time shares that dwarf the competition. Therefore, this paper gives particular regard to regulatory action and engagement involving Google and Facebook.

The overview of enforcement action in Part B identifies the digital platforms that have garnered the attention of regulators. These include Amazon, Apple, Facebook, Google, Grindr, Instagram, LinkedIn, TikTok, Tinder, Twitter, WhatsApp, Yelp, and YouTube.

2.2 Recent developments in Australia

In June 2019, the Australian Competition and Consumer Commission (ACCC) released the report of its Digital Platforms Inquiry into the impact of digital search engines, social media platforms, and digital content aggregators on the state of competition in media and advertising services markets. In that report, the ACCC recommended, amongst other things, that the Privacy Act be reviewed. In

[1] See Australian Competition and Consumer Commission, Digital Platforms Inquiry, June 2019, p 6.

December 2019, the Government agreed to a review of the Privacy Act to ensure privacy settings empower consumers, protect their data and best serve the Australian economy.[2] The Government also committed to increasing penalties and introducing a binding social media and online platforms privacy code.[3]

This paper aims to support the OAIC's internal preparation to contribute to a review of privacy law and development of a privacy code. Its purpose is to provide a strong evidence base upon which the OAIC may develop its policy and regulatory thinking in terms of the unique privacy challenges introduced by digital platforms.

[2] Prime Minister, Treasurer, Attorney-General, Minister for Industrial Relations, Minister for Communications Cyber Safety and the Arts, Media release, *Response to digital platforms inquiry*, 12 December 2019.

[3] Prime Minister, Treasurer, Attorney-General, Minister for Industrial Relations, Minister for Communications Cyber Safety and the Arts, Media release, *Response to digital platforms inquiry*, 12 December 2019.

PART A – KEY PRIVACY REGULATORY ISSUES FOR DIGITAL PLATFORMS

3. Cross border operation

3.1 Challenge posed by digital platforms

The digital economy does not heed borders, yet the laws regulating it do. This blocks effective enforcement as domestic regulators struggle to hold to account organisations based in foreign jurisdictions but trading globally. Regulators face this challenge for all businesses trading online, however, large digital platforms create unique challenges for cross-border enforcement. Social media platforms and search engines often do not charge for use of their platforms and do not deliver goods. Revenue is indirect, through advertising and trading in data. Under some privacy law, this is adequately 'grey' as to create uncertainty about coverage.

Another unique challenge with regard to digital platforms relates to their extensive profiling and advertising activities which effectively moves data across borders and through many sets of hands. The challenge of regulating potentially immense cross-border data flows is exacerbated by such intermediaries and affiliates having only a tenuous relationship with the individual, often at many points of remove. In these circumstances, individuals are unlikely to be aware of the number and identities of these intermediaries and thus unlikely to complain about their conduct. So jurisdictional barriers to enforcement are compounded by minimal awareness of such third-party data handling by individuals. See section 5 (targeted advertising) and section 7 (individual loss of control).

3.2 Regulatory responses

3.2.1 Expansions to extraterritorial operation of privacy regulation

In the past, digital platforms have disputed their coverage under other countries' domestic privacy legislation on the grounds that the platform processed data only in its home jurisdiction. This was Google's argument in the 2014 'right to be forgotten' case in Spain. In that case, the European Court of Justice found that, to the contrary, Google was covered by Spanish data protection legislation since it promoted and sold advertising space in that jurisdiction.[4] Since then, reforms to data protection regulation have deliberately expanded its extraterritorial clout, most notably in the EU via the GDPR, but also in California, Japan and New Zealand. Previously, New Zealand has had difficulty holding Facebook to account with Facebook claiming it was not covered by New Zealand privacy law.[5] The New Zealand Office of the Privacy Commissioner (NZ OPC) has pointed out that its reformed Act (set to take effect in December 2020) will now apply to businesses located offshore like Google and Facebook.[6]

It is not only new and reformed laws, however. The Children's Online Privacy Protection Act (COPPA) has been in force for 20 years and applies to foreign-based websites or online services that are

[4] Court of Justice of the European Union, Press Release no. 70/14, Luxembourg, 13 May 2014.

[5] NZ OPC, Blog, Facebook: What this is really about, 3 April 2018.

[6] NZ OPC, Privacy 2.0: Key changes in the Privacy Act 2020, 16 June 2020.

directed at, or collect the information of, children in the US.[7] The US Federal Trade Commission (FTC) has pursued a number of foreign-based organisations under COPPA in recent years including TikTok and others (see section 18.4).

3.2.2 Restrictions on cross-border disclosure

The EU has long imposed restrictions on transfers of data outside the European Economic Area and this continues under the GDPR. Other jurisdictions do the same, often enabling transfer outside their borders with the individual's consent or where the recipient is bound by appropriate privacy standards. The US does not have a comprehensive data protection law in the traditional sense (see section 18), though other legislation such as COPPA and, in California, the CCPA restrict data sharing (and by implication cross-border sharing), particularly on the request of an individual.

3.2.3 Regulator coordination

There continues to be an emphasis on privacy regulator coordination via agreements, frameworks and networks including the APEC Cross-border Privacy Rules (CBPR) system, Global Privacy Enforcement Network, and the EU-US Privacy Shield Framework. The APEC CBPR system incorporates two elements – a cooperation framework and an enforcement framework. Under this arrangement, economies that wish to be part of the CBPR system must have available a backstop regulator that can bring the force of law to the enforcement of breaches.

In the US, the FTC can cooperate with other data protection authorities under the SAFE WEB Act which allows the FTC to share information with foreign counterparts to combat deceptive and unfair practices.[8] It was under this Act that the FTC collaborated with the UK Information Commissioner's Office in 2019 in its actions against Cambridge Analytica and Aleksandr Kogan and Alexander Nix.[9]

EU data protection authorities also take a coordinated response to GDPR enforcement, with a lead authority making a decision on a matter and then allowing other relevant authorities to submit 'reasoned and relevant objections' should they disagree with the lead authority's reasoning (see section 10.3).

Such cooperation can strengthen the regulatory response to privacy issues arising in multiple jurisdictions, which is common when the issue has to do with digital platforms. However, at times cross-border cooperation significantly extends time taken to complete an investigation. In the EU, the Irish Data Protection Commission is leading a number of inquiries into tech firms, many of which require cross-border coordination with other EU data protection authorities. It seems likely, however, that cross-border inquiry processing time will accelerate once interpretation is settled on key aspects of the GDPR.

---

[7] FTC, Frequently Asked Questions, COPPA Enforcement, B7.

[8] FTC, *2019 Privacy and Data Security Update*, p 18.

[9] FTC, *2019 Privacy and Data Security Update*, p 18.

4. Power asymmetries

4.1 Challenge posed by digital platforms

Some digital platforms are large, both in terms of revenue and numbers of users. This creates the conditions for power asymmetries both between the company and the user, and the company and the regulator. For platforms with a majority market share or near monopoly, like Google, YouTube, Twitter, Facebook and Instagram, the ability of users to exercise their power to choose alternative providers is undermined as alternatives may be scarce – there are few alternatives to YouTube if a person wishes to share videos with a large audience. These conditions entrench the power imbalance because while users may dislike the platform's privacy practices, they cannot 'vote with their feet' and take their business elsewhere.

The power imbalance between users and platform may take the form of knowledge or information asymmetries, where the platform 'knows everything' and the user 'knows nothing'. In the privacy context, this means the platform has a full view of how data is used, processed and disclosed through its service and the user has only a partial view or perhaps no view at all; backend data processing is invisible to them. Information asymmetries put the user at a disadvantage. Users are unable to determine whether their information is being used outside their expectations, let alone seek redress or pursue their information rights.

Data protection laws have sought to correct this asymmetry by requiring organisations to explain their data processing practices in personal information collection notices and privacy policies. However, as the complexity of data processing increases, so does the length and complexity of notices and policies, transforming them into a vehicle for obscurity rather than transparency.

The challenge of releasing meaningful information about data processing is amplified by the particular business model of large 'free' digital platforms which make their revenue from monetising users' data and selling targeted advertising opportunities. This business model requires platforms like Google and Facebook to attract a large number of users and build rich datasets about them.[10] Data about users is collected directly from the platforms and from a vast array of other websites and apps. It is estimated that more than 70 percent of websites have a Google tracker and more than 20 percent of websites have a Facebook tracker.[11]

The associated data processing is extensive and intricate, involving a large number of partners, affiliates and intermediaries. Such complexity necessarily impacts on the effectiveness of privacy notices and policies which attempt accuracy at the cost of clarity and vice versa. Numerous studies have drawn attention to the length and complexity of privacy notices and low rates of notice readership.[12]

---

[10] See Australian Competition and Consumer Commission, Digital Platforms Inquiry, June 2019, p 7.

[11] See Australian Competition and Consumer Commission, Digital Platforms Inquiry, June 2019, p 11.

[12] Katharine Kemp, '94% of Australians do not read all privacy policies that apply to them – and that's rational behaviour', *The Conversation,* 14 May 2018.

New Zealand Privacy Commissioner John Edwards has also highlighted the power asymmetries between the few tech giants and the many and varied jurisdictions and regulators in the world, or what he terms the 'they are one, and we are many' problem. He observes that it is a challenge to coordinate domestically with authorities with a shared interest in regulating digital technologies and platforms:

> When you multiply the challenge across every jurisdiction with a censor, electoral commission, competition authority, consumer protection authority and online harms agency, the scale of the fragmentation becomes immediately evident. Yet They remain One.[13]

The EU has counteracted this disparity through enacting the GDPR across all of its member states so that the 'we are many' problem becomes 'we are many acting as one.' Certainly, the GDPR has become a global benchmark for data protection – a single domestic data protection law could not have achieved the same impact. The EU has also sought to rebalance the power asymmetry between regulators and the tech giants through significantly increasing the fines for non-compliance. Beefing up fines and regulator enforcement powers has been a theme across a number of jurisdictions.

However, Edwards raises a more nuanced point which goes to the diversity of cultural mores and values. Much of the privacy debate over the past two decades has focused on fostering consistency of privacy regulation across jurisdictions to make compliance easier for organisations. What this may result in is countries setting aside their own cultural mores and values (which would otherwise justify variation in the scope or emphasis of domestic privacy law) for the convenience of a single system.

4.2 Regulatory responses

4.2.1 Focus on transparency

To rebalance the information asymmetry, most privacy laws contain transparency provisions requiring organisations to publish information about their collection and handling of personal information. Many jurisdictions now also mandate breach reporting.[14] California has a number of additional transparency measures in place, including laws requiring online publication of a data broker register, online publication of privacy policies, and disclosure (on request) of what personal information an organisation has shared and with whom (see section 8).

Additionally, privacy regulators have focused on transparency obligations in recent enforcement actions against digital platforms. For example, the FTC found that Facebook's privacy settings were misleading (implying less data sharing than was actually the case) (see section 18.2). Under the GDPR, controllers must give data subjects certain information about their collection and use of the person's personal data including the 'legal basis for processing'. Several of the inquiries currently on foot involving data platforms involve an examination of the platform's transparency on this point.[15] In

---

[13] John Edwards, New Zealand Privacy Commissioner, 'Addressing the Power Asymmetry of the Big Technology Companies', keynote address to the IAPP ANZ Summit, 30 October 2019.

[14] See for example, Australia, California, Canada, EU (GDPR), Japan, New Zealand, Singapore (proposed).

[15] See, for example, Irish Data Protection Commission inquiries into Instagram, Facebook and WhatsApp (see section 10).

its case against Google, the French privacy regulator, CNIL, found that Google had not met transparency obligations as essential information about data processing purpose, the data storage periods and the categories of personal data used for ad personalisation was excessively disseminated across documents and webpages.[16] CNIL also found the information to be not always clear and comprehensive, with information about collection purpose described in a 'too generic and vague manner.'

The FTC Facebook case also gave attention to transparency of privacy management with the order imposed on Facebook requiring specific actions to increase openness of how it manages privacy and complies with its privacy obligations under the order. This includes a number of lines of reporting (including to the FTC) such as quarterly compliance certification; biennial independent assessments; quarterly reporting of the independent assessor to Facebook's board privacy committee; quarterly reporting of privacy reviews; and breach reporting to the FTC. The FTC's reported intention was to create 'an unprecedented level of transparency for Facebook's privacy practices'[17] (see section 18.2).

The GDPR also seeks to strengthen public accountability by requiring certain organisations to appoint a data protection officer (DPO), publish their contact details and provide them to the relevant data protection authority. Specifically, organisations whose core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking) must appoint a DPO – a provision that appears to target digital platforms.[18]

4.2.2 Stronger privacy management and governance

Other jurisdictions have sought to enhance the rigor of privacy compliance and management. In India, a new privacy bill proposes that 'significant data fiduciaries' (a category of 'controller' that is likely to include large digital platforms) must submit their processing to annual audit by independent auditors (see section 12). In the EU, the GDPR requires data protection impact assessments (DPIAs) in certain circumstances, including where a controller wishes to use systematic and extensive profiling with significant effects.[19] The UK Information Commissioner's Office (ICO) has further specified that in its jurisdiction, controllers must also conduct a DPIA for projects involving: profiling of individuals on a large scale, matching data or combining datasets from different sources, collecting personal data from a source other than the individual without providing them with a privacy notice ('invisible processing'), tracking individuals' location or behaviour, and profiling children or targeting marketing or online services at them.[20]

The Irish DPC has actively engaged platforms on the DPIA requirement, recently raising concerns about the fact Facebook had failed to provide it with documentation concerning any DPIA or decision-

---

[16] French National Data Protection Commission (CNIL), The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019.

[17] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 3.

[18] See UK Information Commissioner's Office, Guide to the GDPR.

[19] UK Information Commissioner's Office, Guide to the GDPR.

[20] UK Information Commissioner's Office, Guide to the GDPR.

making processes undertaken in relation to a proposed new dating feature.[21] Following the DPC's intervention, Facebook opted to postpone roll-out.

4.2.3 Increases in fines and stronger regulator powers

New and reformed privacy laws have strengthened regulator powers and increased the size of penalties available under them. Most notably, the GDPR allows regulators to impose a fine of €20 million or 4 percent of annual worldwide turnover, whichever is higher. So far, the highest fine imposed under the GDPR was €204 million against British Airways. The highest GDPR fine against a *digital platform* was €50 million imposed by the French data protection authority on Google.

The FTC, which has not had any significant change to its powers or penalty provisions, has also broken records with its recent $5 billion USD penalty against Facebook (a penalty 20 times larger than CNIL's penalty imposed on Google). Further, the FTC's $170 million USD fine against YouTube for COPPA violations also broke records, being higher than any previous COPPA penalty by a factor of 30. This implies that, even without legislative change, there is a recognition of the need for a change in approach when it comes to the tech giants. Commenting on the Facebook case, the FTC commissioners supporting the settlement stated: 'The magnitude of this penalty resets the baseline for privacy cases—including for any future violation by Facebook—and sends a strong message to every company in America that collects consumers' data: where the FTC has the authority to seek penalties, it will use that authority aggressively.'[22]

Discussion about the appropriate size of fines against digital platforms is ongoing. Despite the record-breaking size of the Facebook fine, dissenting FTC Commissioner Slaughter pointed out that 'as of [2019], Facebook brings in around $5 billion on a monthly basis.'[23] Dissenting FTC Commissioner Chopra also stated that 'even if $5 billion were a reasonable estimate of Facebook's unjust gains [Chopra claims it is not], it would be inadequate as a civil penalty. A civil penalty should exceed unjust gains – otherwise we are allowing a defendant to break even or even profit by breaking the law.'[24]

---

[21] See Irish Data Protection Commission, Statement on Facebook dating feature, 12 February 2020.

[22] See Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson re Facebook, Inc. July 24, 2019, pp 1-2.

[23] Dissenting Statement of Commissioner Rebecca Kelly Slaughter in the matter of Facebook, 24 July 2019, p 8.

[24] Dissenting Statement of Commissioner Rohit Chopra in re Facebook, 24 July 2019, p 16.

5. Targeted advertising and digital tracking

5.1 Challenge posed by digital platforms

The privacy risks arising in connection with profiling, tracking and targeted advertising are now a central concern for many jurisdictions. The amount of data collected, shared, analysed and manipulated is difficult to comprehend. Online tracking can be particularly privacy-impactful because it operates far beyond the confines of a single platform. The ACCC examined this issue in detail in its Digital Platforms inquiry and so IIS will not repeat its findings here.

Other jurisdictions have also raised concerns. FTC Commissioner Rohit Chopra has commented on the way that large platforms take advantage of the breadth of their market share: 'As a subsidiary of Google, YouTube is not an independent company. Google uses insights from other properties to enhance its targeting and monetization of YouTube, and it uses YouTube viewing behavior to better monetize its other properties. Tracking users across properties makes all of the properties more valuable, since the detailed data collected on each user can be used to induce them to watch or click on ads.'[25]

The UK ICO has given particular attention to the adtech industry, conducting a long-running investigation of the practice of real-time bidding (RTB) and its privacy implications. The ICO has sought to address the significant lack of transparency of RTB due to the nature of the supply chain and the many different actors and service providers that sit between the advertisers buying online advertising space, and the publishers selling it.[26] The ICO set RTB against the requirements of the GDPR – particularly requirements related to transparency, lawful basis for processing and security.[27]

Targeted advertising and digital tracking raise issues that compound privacy risks:

- **A business model that encourages data maximisation**
  There is an impetus on platforms to collect, use and share as much user personal information as possible to support advertising activities.
- **Complex information ecosystem and difficulties maintaining oversight over all players**
  Where there is a complex information ecosystem, platforms may be unwilling to accept responsibility for the actions of partners, affiliates, app developers, data brokers, advertisers and others, particularly where oversight is expensive and where lack of oversight or enforcement has a financial benefit for the platform.[28]

---

[25] Dissenting statement of Commissioner Rohit Chopra in the matter of Google and YouTube, 4 September 2019, p 4.

[26] UK Information Commissioner's Office, *Blog: Adtech - the reform of real time bidding has started and will continue*, 17 January 2020.

[27] See UK Information Commissioner's Office, Update report into adtech and real time bidding, 20 June 2019 p 15.

[28] For an example of this, see section 18.2.1.

- **Lack of clarity in privacy settings and notices to serve business outcomes**
  Given the 'data maximisation' business model, platforms are incentivised to configure privacy settings in a way that encourages permissive information sharing, for example through unclear information about how the settings work, permissive default settings, opt out instead of opt in, and scattering privacy controls and privacy information across a number of different pages to make it difficult for users to get a complete view of the platform's handling of their data.[29]
- **Lack of transparency coupled with business imperatives raises ethical questions**
  The sudden and rapid development of the digital sector means digital platforms may face ethical questions that are novel and that society has not yet found an answer to. Regulations intended to apply a form of brake on platform data processing may be ineffectual where technological change has out-paced legislative reform.

5.2 Regulatory responses

5.2.1 Expansions to definition of personal information

Some jurisdictions have expanded or specifically worded their definition of personal information in a way to ensure that online tracking and profiling is covered by privacy law. In the US, the FTC amended rules under the Children's Online Privacy Protection Act (COPPA) in 2013 to expand the definition of personal information to cover a persistent identifier that can be used to recognise a user over time and across different sites, including a cookie number, an IP address, a processor or device serial number, or a unique device identifier. It was also expanded to cover geolocation information sufficient to identify a street name and city or town.[30]

The newly enacted California Consumer Privacy Act (CCPA) has a broad definition of personal information. It is defined as 'information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.' The CCPA also provides specific categories that are considered personal information, which include categories of information that appear to target information collected in the course of online tracking and profiling. This includes 'online identifier', 'IP address' and 'geolocation data', along with 'Internet or other electronic network activity information that includes browsing history, search history and information regarding a consumer's interaction with an Internet Web site, application or advertisement'. The definition of personal information also covers: 'Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities and aptitudes.'

The GDPR defines personal data as 'any information relating to an identified or identifiable natural person'. It further specifies that 'an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location

[29] For an example of this, see section 10.6.1.

[30] See FTC, *COPPA: Six Step Compliance Plan for your Business*.

data, an online identifier…'[31] The UK ICO has advised that 'online identifiers' includes IP addresses and cookie identifiers.

5.2.2 Enforcement focus on targeted advertising

Many of the enforcement actions on foot in the EU are examining the 'legal basis for processing' in the context of targeted advertising. Under the GDPR, controllers are required to disclose the legal basis for processing. There are six lawful bases for data processing, one of which is data subject consent, another of which is the controller's 'legitimate interest'.[32] The UK ICO has examined the 'legitimate interests' basis as it applies to RTB. It found that, although it had 'reviewed a number of justifications for the use of legitimate interests as the lawful basis for the processing of personal data in RTB [its] current view is that the justification offered by organisations is insufficient.'[33]

In the French data protection authority's (CNIL) case against Google, CNIL found that Google violated its obligation to have a legal basis for processing personal information. Google stated that it obtained the user's consent to process data for ads personalisation purposes and that this was its legal basis for processing. However, CNIL found that the consent was not validly obtained because users' consent was not sufficiently informed and users' consent was neither specific nor unambiguous.

Other cases examining the legal basis for data processing in the context of targeted advertising are currently on foot in the EU. These include inquiries into the practices of Apple, Facebook, LinkedIn and WhatsApp.

5.2.3 Right to object

Expansions of individual rights including the right to object strengthen the ability of individuals to stop their data from being used for targeted advertising. The GDPR gives individuals an absolute right to stop their data from being used for direct marketing and California has given consumers the right to demand that organisations covered by the California Consumer Privacy Act not sell their personal information (see section 7.2.1).

---

[31] See General Data Protection Regulation, Article 4.

[32] See UK Information Commissioner's Office, Guide to the GDPR, for an explanation of the 'legitimate interests' legal basis for processing.

[33] UK Information Commissioner's Office, *Blog: Adtech - the reform of real time bidding has started and will continue*, 17 January 2020.

6. Challenge of meaningful consent

6.1 Challenge posed by digital platforms

Requiring organisations to seek individuals' consent to use their personal information in certain circumstances is a feature of most privacy law. Consent requirements aim to give individuals more choice and control over the handling of their information. Asking for permission to collect personal information is a form of respect for the individual – an acknowledgement that the information is theirs and they deserve to direct how it is used. However, the digital age has put additional pressure on consent as a mechanism for individual control. The utility of personal data has skyrocketed and, with it, the amount of data collected and processed. In practical terms, this means that individuals are being asked for consent to use their data much more frequently than in the pre-digital era. Add to this the complexity of much personal data processing, and the result is that individuals are under pressure like never before to understand complex processing and to agree to it.

The challenge is more acute in relation to the data processing practices of digital platforms because the data processing that supports targeted advertising is highly complex. It is difficult in these circumstances for an individual to give meaningful consent because it is difficult for them to be meaningfully informed. Part of the issue is one of competence and whether it can be said that individuals are qualified and competent to understand and agree to complex processing involving their data. Consent is also difficult in the digital platform context because of the monopoly many platforms have in their corner of the market. This may undermine the 'free' aspect of consent, where the options – consent to the terms and conditions and create an account or do not consent and therefore do not use the platform – are not really options at all where there is no alternate platform.

Given these challenges, it is interesting to observe the actions of other data protection authorities as they test consent requirements via enforcement action. After all, consent continues to be a feature of most privacy law, though it is not usually a blanket requirement. For example, under the GDPR, having the individual's consent is one of six lawful bases for data processing. The UK ICO advises that '[c]onsent is not inherently better or more important than [the] alternatives. If consent is difficult, you should consider using an alternative [lawful basis].'[34] In contrast to an approach that sees consent as the first choice for lawful basis for processing, the ICO implies that actually it should be the last. In its *Guide to the GDPR*, it notes that 'You are likely to need to consider consent when no other lawful basis obviously applies.'[35] Concerning 'special category data', the ICO notes that 'alternative conditions for processing [this] data are generally more restrictive and tailored to specific situations, but you should still check first whether any of them apply.'[36] Furthermore, 'If you make consent a precondition of a service, it is unlikely to be the most appropriate lawful basis.'[37]

---

[34] UK Information Commissioner's Office, Guide to the GDPR / Lawful basis for processing / Consent.

[35] UK Information Commissioner's Office, Guide to the GDPR / Consent / When is consent appropriate?.

[36] UK Information Commissioner's Office, Guide to the GDPR / Consent / When is consent appropriate?.

[37] UK Information Commissioner's Office, Guide to the GDPR / Lawful basis for processing / Consent.

6.2 Regulatory responses

6.2.1 Requiring simple consent withdrawal

The GDPR gives individuals an explicit right to withdraw consent at any time. Being able to withdraw consent has long been considered an inherent aspect of valid consent, however this marks a change whereby the requirement to allow withdrawal of consent is enshrined in the statute itself. Further, Article 7(3) of the GDPR specifies that '[i]t shall be as easy to withdraw as to give consent.' The UK ICO has advised that 'the process of withdrawing consent should be an easily accessible one-step process.' Further, '[a]s the right to withdraw is 'at any time', it's not enough to provide an opt-out only by reply. The individual must be able to opt out at any time they choose, on their own initiative.'[38]

An explicit right to withdraw consent significantly strengthens the control individuals have over their data. This is particularly relevant in the context of targeted advertising given the UK ICO has found that the adtech industry should be getting consent to process data for RTB (see section 17.3). It is also relevant for other recent enforcement actions (such as CNIL's inquiry into Google) where the platform has argued that it processes data for ad personalisation with consent (see section 10.6.1). In these cases, the GDPR would appear to give individuals a clear right to withdraw consent to such processing. It also implies that platforms must make consent withdrawal 'an easily accessible one-step process.'

6.2.2 Enforcement focus on consent

A number of recent and ongoing enforcement cases involving digital platforms have examined consent and shortfalls in consent, particularly in the EU. In the case mentioned above, the French data protection authority, CNIL, found that Google had not obtained valid consent to use individual's data for ad personalisation because users were not adequately informed, and consent was not adequately specific or unambiguous (see section 10.6.1).

Other GDPR inquiries into digital platforms are considering the related issue of 'lawful basis' for processing, and whether consent is both the appropriate basis and has been conducted in according with GDPR consent requirements. These cases have particularly focused on processing for the purpose of targeted advertising. See, for instance, cases currently on foot involving Apple, Facebook, LinkedIn, Tinder and WhatsApp (see section 10). The outcomes of these various actions will test GDPR consent requirements and offer guidance on how EU authorities intend to enforce consent standards in relation to digital platforms.

[38] UK Information Commissioner's Office, Guide to the GDPR / Consent / How should we obtain, record and manage consent?.

7. Individual loss of control over personal information

7.1 Challenge posed by digital platforms

Digital platforms make most of their revenue from advertising and therefore rely on extensive data collection and processing to enable better targeting of ads to the interests of users. Much of this processing is invisible to the individual. Recent enforcement action by the FTC against Facebook and Google also reveal the way that platforms have misled users about privacy settings and how they share personal data. The 'data maximisation' business model incentivises platforms to configure privacy settings in a way that encourages permissive information sharing, for example through unclear information about how the settings work, permissive default settings, opt out instead of opt in, and scattering privacy controls and privacy information across a number of different pages to make it difficult for users to get a complete view of the platform's handling of their data.

The invisibility of such data processing and the complexity of data supply chains, coupled with difficulty getting a complete picture of platform data sharing arrangements, may create obstacles to individuals being able to manage their privacy.

7.2 Regulatory responses

7.2.1 Expanded data rights for individuals

A number of jurisdictions have expanded the rights available to individuals under privacy law – most notably, the EU which has introduced a wide-range of rights including the right to be informed, the right to erasure (also known as the 'right to be forgotten'), the right to restrict processing, and the right to object. (See section 10.2 for a full list of GDPR rights.) Most of these rights include exceptions, though the GDPR gives individuals an absolute right to stop their data from being used for direct marketing. Other jurisdictions have legislated a 'right to be forgotten'. And California has given consumers the right to demand that organisations covered by the California Consumer Privacy Act not sell their personal information. Accompanying this provision is the requirement that organisations not discriminate against consumers who exercise the right.

In addition to expanding data rights for individuals, the GDPR also requires organisations to make it easy to withdraw their consent to data processing (see ection 6.2.1).

7.2.2 Transparency requirements

Regulators have also given particular attention to compliance with transparency obligations and identifying misleading privacy information (see section 4.2.1).

PART B – OVERVIEW OF REGULATORY APPROACHES BY JURISDICTION

8. California

The recently enacted California Consumer Privacy Act (CCPA) has created waves in the US and globally due to its strict privacy rights and obligations. Certainly, it is the first law of its kind in the US, though there are indications that other states will follow California's lead. It imports a number of GDPR-like rights into Californian law, marking a departure from the non-privacy-specific 'consumer protection' bent of regulation at the federal level.

It is not the first time California has set precedents for regulating privacy rights online, with earlier laws – the California Online Privacy Protection Act and Shine the Light Act – addressing particular privacy issues arising in the digital age. This makes California a jurisdiction of interest for a study of digital platforms and privacy. Many of the same themes emerge as in other jurisdictions: extraterritorial operation of legislation, broader definitions of personal information, and stronger individual rights. Additionally, though, we see early attempts to manage, or at least make transparent to consumers, online tracking across websites and platforms.

8.1 California Consumer Privacy Act

The CCPA reflects many trends noticeable in other jurisdictions including a broad definition of personal information (that specifically incorporates data involved in online profiling and targeted advertising), extraterritorial operation and expanded rights for individuals.

8.1.1 Definition of personal information

The CCPA has a broad definition of personal information. It is defined as 'information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.' The CCPA also provides specific categories that are considered personal information, which include:

- **Identifiers** such as real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's licenses number, passport number or other similar identifiers
- **Commercial information**, including records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies
- **Biometric information** which is defined as 'an individual's physiological, biological, or behavioural characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity'
- **Internet or other electronic network activity information** that includes browsing history, search history and information regarding a consumer's interaction with an Internet Web site, application or advertisement
- **Geolocation data**
- **Audio, electronic, visual, thermal, olfactory**, or similar information

- **Professional or employment related information**
- **Education information**, provided that it is no publicly available and
- **Inferences** drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities and aptitudes.

This definition is broader and more complex than the definition of personal data under the GDPR. It covers information that identifies a consumer along with information that 'relates to' a consumer which implies a lower bar. Notably, many of the specific categories of information listed appear to target information collected in the course of online tracking and profiling.

The CCPA does not apply to de-identified information or aggregate consumer information and also excludes medical information from its protection (which is covered by separate regulations). The CCPA defines de-identified information as 'information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

1. Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
2. Has implemented business processes that specifically prohibit reidentification of the information.
3. Has implemented business processes to prevent inadvertent release of deidentified information.
4. Makes no attempt to reidentify the information.'[39]

8.1.2 Extraterritorial operation

To be covered by the CCPA, an organisation must (among other things):

- Collect personal information from California residents
- Determine the purposes and means of the processing of that information (in other words: is a 'controller' rather than a 'processor' of data in the GDPR sense)
- Do business in California.

The CCPA does not provide a precise definition of what 'doing business in California' means. Many point to Californian taxation law which states that 'a business is doing business in California if it actively engages in any transaction for the purpose of financial or pecuniary gain or profit in California.' This appears to indicate that CCPA would cover a business not located in California that otherwise targets Californian residents or that conducts online transactions with California residents.

---

[39] Cal. Civ. Code § 1798.140(h).

8.1.3 Consumer rights

The law gives consumers powers over their data. The new rights are as follows:

- The right to access personal information allows consumers to ask to see the details of the data that businesses have on them. They are also entitled to see the categories of personal data that are held and the right to see specific inferences that have been made about them which may include predictions and categorisations. Moreover, consumers also have the right to know what kind of third parties a company has obtained their information from or sold it to.
- The right to delete personal information gives consumers the right to request for the deletion of their personal data. However, this is not an absolute right as certain exceptions may apply.
- The right to be informed places the obligations on the business to inform consumers of the categories of personal information that are being collected, the purpose of collecting that information, the categories of sources from which the personal information is collected, and the categories of third parties with whom the business shares personal information.
- The right to object (opt-out) essentially gives consumers the authority to decide to opt-out from the selling of their personal information. If a business sells consumers' personal information, information about this right must be given to consumers in the privacy notice. Moreover, a link to the page 'Do Not Sell My Personal Information' must be included in the homepage of the business.

Access and information rights have existed in privacy law in other jurisdictions for some time now. However, the right to delete personal data and the right to object, are relatively new data rights and to some extent correspond to similar rights under the GDPR. The right to delete personal data is, as noted above, subject to exceptions. Consumers can exercise this right if:[40]

- the personal information was collected by the business from the individual and
- it is no longer necessary for the business or service provider to maintain the personal information to fulfill one of the purposes identified in Cal. Civ. Code Sec. 1798.105 (d) and
- the business is not entitled to retain the personal information under one of the general exemptions in the CCPA (see Cal. Civ. Code Sec. 1798.145).

The purposes outlined in section 1798.105 (d) are broad and would appear to significantly limit the operation of this right in practice. For example, a business may refuse a 'delete request' if the business needs to maintain the consumer's personal information to use it, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.

8.2 California Privacy Rights Act

In May 2020, Californians for Consumer Privacy, the group behind the ballot initiative that inspired the CCPA announced that it had collected over 900,000 signatures to qualify the California Privacy Rights

[40] See Lydia F de la Torre, 'The right to delete', *Medium,* 6 April 2020.

Act (CPRA) for the November 2020 ballot.[41] The CPRA is an update to the California Privacy Rights and Enforcement Act (CPREA) ballot initiative, which was proposed in late 2019. The CPRA would amend the CCPA to create new and additional privacy rights which include:

- **Sensitive personal information –** a new category of 'sensitive personal information' would be established which would cover many of the same types of information as are covered under the concept of 'sensitive information' in Australian law. Notably it will include 'precise geolocation'.
- **Right of correction –** Californian consumers would be granted the right to request the correction of their personal information if that information is inaccurate.
- **Children's data –** the CPRA purports to enhance children's privacy by tripling fines for violations of the CCPA's opt-in to sale right and creating a new requirement to obtain opt-in consent to sell or share data from consumers under the age of 16.
- **Data breach liability provision –** the CPRA would amend the CCPA's data breach liability provision to clarify that breaches which result in the compromise of a consumer's email address in combination with a password or security question and answer that would permit access to the consumer's account are subject to the relevant provision.
- **Limited retention –** the CPRA expressly limits a business's ability to retain personal information as 'necessary and proportionate' to achieve the purposes of collection or processing, or for other disclosed purposes compatible with the context of collection.
- **Express information security requirements –** businesses must 'implement reasonable security procedures and practices.'
- **Enforcement –** an Agency called the California Privacy Protection Agency would be established to enforce the law.

8.3 Other transparency measures

8.3.1 Law requiring registration of data brokers

As of the beginning of 2020, Californian law requires data brokers to register with the Attorney General and for the Attorney General to make available online a list of registered brokers.[42] Under the legislation 'data broker' is defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship.[43]

Explanatory material associated with the data broker bill noted that although the CCPA 'provided ground-breaking rights for consumers to protect their right to privacy, many of the CCPA's provisions require consumers to know which entities have their personal information before they can properly exercise their rights.'[44] This is difficult in the data broker context because data brokers, by definition,

---

[41] 'Californians for Consumer Privacy introduces California Privacy Rights Act for November 2020 ballot,' *Hunton Privacy Blog,* 4 May 2020.

[42] For the list of data brokers, see State of California Department of Justice, *Data Broker Registry*.

[43] Senate Floor Analyses, AB 1202, Third Reading, 10 September 2019, p 2.

[44] Senate Floor Analyses, AB 1202, Third Reading, 10 September 2019, p 5.

do not have a direct relationship with the individual. Requiring data broker registration and offering a public list of data brokers, their websites and contact details aims to improve transparency and better allow privacy conscious consumers to exercise their rights granted under the CCPA.[45]

8.3.2 California Online Privacy Protection Act

California enacted the Online Privacy Protection Act (CalOPPA) in 2003. The Act requires operators of commercial websites that collect personal information of Californian residents to post (and comply with) a privacy policy.[46] CalOPPA specifies what information the privacy policy must include.

The scope of CalOPPA is broad: it covers operators whose website is accessible to Californians – neither the operator nor its servers need to be based in California.

8.3.3 California Shine the Light Law

The California Shine the Light law was enacted in 2003 and came into force in 2005. Its purpose was to improve transparency of sharing of personal information for marketing purposes and allows Californian residents to ask what personal information an organisation has shared with third parties and which third parties it was shared with. Organisations are exempt from complying with a request for this information if they offer Californian residents an option to opt-out of having their data shared. It is not clear whether the CCPA (which requires organisations to offer consumers a 'do not sell my personal information' option) has overtaken the Shine the Light law. Regardless, this law indicates that California has taken a long-running interest in managing the privacy risks associated with data brokerage and use of personal information for marketing.

---

[45] Senate Floor Analyses, AB 1202, Third Reading, 10 September 2019, p 6.

[46] See Business and Professions Code, s 22575.

9. Canada

Canada has two federal privacy laws. The Personal Information Protection and Electronic Documents Act (PIPEDA) was enacted in 2000 and applies to the collection, use or disclosure of personal information in the course of a commercial activity. And the Privacy Act, which applies to government departments and agencies.

In 2018, in the wake of the Cambridge Analytica-Facebook scandal, the government expanded rules under PIPEDA requiring businesses to report to the Office of the Privacy Commissioner of Canada (OPC) and affected individuals when a data breach involving 'a real risk of significant harm' to individuals has occurred.[47] Canada will be a jurisdiction to monitor as it reforms its privacy regime in light of technological change.

9.1 Legislative reform and Digital Charter

In light of continuous developments of privacy and data protection laws globally, Canada is planning to revamp its laws. In 2019, the Canadian government introduced a Digital Charter.[48] The Digital Charter outlines what Canadians can expect from the federal government in relation to the digital landscape. As part of the effort to implement the principles of the charter, the government is planning to reform and modernise PIPEDA. The government's plan is focused on the following four areas:[49]

- Enhancing individuals' control as digital platforms and services continue to become an integral part Canadians' daily life.
- Enabling responsible innovation to ensure that there is increased accountability and higher standards of care for privacy and security in the pursuit of innovative products and services.
- Enhancing enforcement to incentivise compliance and to ensure that there are real consequences when the law is not followed.
- Clarifying responsibilities and obligations in PIPEDA to strengthen accountability.

9.2 Enforcement against Facebook

As the government works on reforming the law, the OPC has continued to carry out its role promoting privacy and ensuring compliance. Most recently, earlier this year, the OPC took regulatory action in relation to the Cambridge Analytica incident, filing a notice of application in the Federal Court that sought a declaration that Facebook had contravened PIPEDA and various orders that would compel Facebook to bring itself into compliance.[50] This application is a result of a joint investigation between

---

[47] Office of the Privacy Commissioner of Canada, News release, 'New data breach reporting requirements come into force this week', 29 October 2018.

[48] M Scherman and M Caldwell, 'Canadian Government announces new digital charter', *McCarthy Tetrault*, 21 May 2019.

[49] Government of Canada, *Strengthening privacy for the digital age*, 21 May 2019.

[50] M Warburton, 'Canadian agency asks federal court to declare Facebook contravened privacy law,' *Reuters*, 7 February 2020.

the OPC and the Information and Privacy Commissioner of British Columbia against Facebook's privacy practices where it disclosed users' personal information to a third-party application without consent.[51] In 2019, the OPC released the findings of the investigation:

- Facebook failed to obtain valid and meaningful consent of installing users.
- Facebook failed to obtain meaningful consent from friends of installing users as it relied on overbroad and conflicting language in its privacy communications that was clearly insufficient to support meaningful consent. It also further relied, unreasonably, on installing users to provide consent on behalf of each of their friends, often counting in the hundreds, to release those friends' information to an app, even though the friends would have had no knowledge of that disclosure.
- Facebook had inadequate safeguards to protect user information.
- Facebook failed to be accountable for the user information under its control and did not take responsibility for giving real and meaningful effect to the privacy protection of its users.

The OPC stated that, during the investigation, Facebook failed to provide evidence about its specific and current personal information handling practices sufficient to satisfy it of Facebook's compliance with PIPEDA. Further, Facebook disputed the investigation report's findings and refused to implement the report's recommendations. As a result, the OPC states in its Application to the Federal Court that until Facebook corrects its practices, there remains a risk that Canadians' personal information will be disclosed or used in ways that users do not know about or expect.

[51] Office of the Privacy Commissioner of Canada, Joint investigation of Facebook, Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia, 25 April 2019.

10. EU and GDPR

The EU's adoption of the GDPR in 2018 has had a major impact on the international regulatory landscape. Many of its features particularly target, or have particular relevance for, digital platforms. For example, the 'right to be forgotten' comes directly from a European Court of Justice case involving Google. The expansion of individual rights under GDPR – including the right to erasure and to object to data processing (which includes an absolute right to stop one's data from being used for direct marketing) – also have significant implications for digital platforms that receive revenue from advertising.

Other more traditional provisions – such as those aimed at data minimisation, security and transparency – also impact digital platforms, and indeed, early enforcement action under the GDPR has involved alleged non-compliance with security and transparency requirements.

This section does not go over the detail of GDPR requirements – such information is available elsewhere. It does, however, identify aspects of the regulation of relevance to digital platforms. It also outlines GDPR enforcement activity involving digital platforms, noting that many of the regulator investigations are ongoing at the time of writing.

10.1 General Data Protection Regulation (GDPR)

In 2016, the European Union (EU) adopted the GDPR, replacing its 1995 European Data Protection Directive (Directive 95/46/EC). In 2012, the European Commission proposed a comprehensive reform of the EU directive.[52] This consideration for reform is what led to the creation of the GDPR. The regulation was created to meet certain objectives:

- To modernise the data protection rules in Europe
- To provide more protection and strengthen the privacy rights of European citizens
- To harmonise the data protection laws of the 28 member states.

The GDPR came into force in May 2018. The comprehensive regulation raised the bar for data protection laws around the world, not only because it gives more rights to individuals but also because it imposes hefty fines in cases of a breach. More importantly, the regulation's extraterritorial reach means it will affect more overseas organisations and, of particular relevance to this study, it will affect digital platforms that are not necessarily based in the EU.

Since its implementation in 2018 and in light of its extraterritorial reach, a number of digital platforms have been fined under the GDPR.

10.2 Individual rights under the GDPR

The GDPR expands the rights available to individuals. Those rights include:

[52] European Data Protection Supervisor, *The History of the General Data Protection Regulation*.

- **Right to be informed** – gives individuals the right to be informed about the collection and use of their personal data.[53]
- **Right of access** – allows individuals to request (verbally or in writing) access to personal data held about them.
- **Right of rectification** – gives individuals the right to have inaccurate personal data rectified or completed if it is incomplete.
- **Right to erasure** – allows individuals to ask for personal information about them to be erased – this right is also known as the 'right to be forgotten'.
- **Right to restrict processing** – allows individuals to ask that a data controller restrict or suppress their personal data. In these circumstances, a controller can store personal data but not use it.
- **Right to data portability** – allows individuals to obtain and reuse their personal data for their own purposes across different services and IT environments. This right only applies to information an individual has provided to a controller.
- **Right to object** – gives individuals the right to object to the processing of their personal data in certain circumstances – this includes an absolute right to stop their data from being used for direct marketing.
- **Rights related to automated decision-making including profiling** – these include requirements for controllers to make it easy for individuals to request human intervention or challenge a decision.

Perhaps the most famous 'right' under the GDPR is the right to erasure or 'right to be forgotten' which arose from a case against Google in Spain in 2014. In that case, the European Court of Justice ruled that European Citizens had a right to request that commercial search firms, such as Google, that gather personal information for profit should remove links to private information when asked, provided the information is no longer relevant.[54] The Court found that the fundamental right to privacy was greater than the economic interest of a commercial firm and, in some circumstances, the public interest in access to information. The case also set a precedent in terms of coverage of an American company by European law. At the time, the European Commission's Vice President Vivian Reding said the decision meant US firms 'can no longer hide behind their servers being based in California or anywhere else in the world'.[55]

There is some cross-over between the right to rectification, the right to restrict processing and the right to object. The right to restrict processing usually does not operate indefinitely but for a period of time to allow resolution of another matter. For example, individuals can ask an organisation to restrict

---

[53] For guidance and commentary on the right to be informed, see the Article 29 Data Protection Working Group, Guidelines on Transparency, 11 April 2018 (which have been endorsed by the European Data Protection Board); see also guidance from the UK Information Commissioner's Office including the Guide to the GDPR and the Guide to the right to be informed.

[54] See European Court of Justice, Judgment in the case of Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 14 May 2014.

[55] David Lee, 'What is the 'right to be forgotten'?', *BBC News*, 13 May 2014.

processing while the organisation processes a rectification request or objection request. Specifically, individuals have the right to request restriction of the processing of their personal data in any of the following circumstances:[56]

- The individual contests the accuracy of their personal data and the organisation is verifying the accuracy of the data.
- The data has been unlawfully processed (in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead.
- The organisation no longer needs the personal data but the individual needs them to keep it in order to establish, exercise or defend a legal claim.
- The individual has objected to the organisation processing their data, and the organisation is considering whether its legitimate grounds override those of the individual.

10.3 Coordinated enforcement

Each member state must establish a data protection authority to enforce the GDPR. For cross-border investigations, the EU takes a coordinated response to GDPR enforcement, with a lead data protection authority making a decision on a matter and then allowing other relevant authorities to submit 'reasoned and relevant objections' should they disagree with the lead authority's reasoning.

In instances where there is disagreement between data protection authorities on a decision, the GDPR contains a dispute resolution mechanism which requires the involvement of the European Data Protection Board (EDPB) to make a final decision on a majority basis.[57]

In the overview of GDPR enforcement actions below, many cross-border investigations are being led by the Irish Data Protection Commission (DPC). This is because many of the tech giants have their EU operations headquartered in Ireland, meaning that complaints against these tech companies in other EU jurisdictions tend to be referred to the Irish DPC. At the close of the 2019 calendar year, the Irish DPC had numerous investigations on foot involving Google, Facebook, Apple, Instagram, WhatsApp, Twitter and others. They are a data protection authority to watch in coming months as they move to finalise these investigations, in consultation with other EU authorities.

10.4 GDPR enforcement against Apple

10.4.1 Ireland

The Irish DPC had two investigations into Apple open at the time of writing.[58]

The second is assessing Apple's compliance with GDPR **access obligations**. The complainant in the case was dissatisfied with Apple's response to their request for access to customer service records.

---

[56] See UK Information Commissioner's Office, Guide to the GDPR.

[57] Natasha Lomas, 'First major GDPR decisions looming on Twitter and Facebook', *TechCrunch*, 23 May 2020.

[58] Irish Data Protection Commission, *2018-2020 Regulatory Activity under GDPR*, 23 June 2020.

Apple claims that the request was 'manifestly excessive'. The DPC is examining whether the access request meets the 'manifestly unfounded or excessive' exception in the GDPR.[59]

The third matter involves assessing Apple's **legal basis for processing in context of behavioural analysis and targeted advertising to users**. The issues under investigation include whether or not the processing of personal data is supported by a legal basis and, if so, which one. This investigation, which follows a complaint made to the French data protection authority, CNIL, appears to raise similar issues to CNIL's case involving Google (see section 9.6.1). Another complaint to CNIL on the same issue has been made concerning Facebook.

10.5 GDPR enforcement against Facebook

10.5.1 Germany

Facebook's German unit was fined 51,000 euros ($55,500) for **failing to properly nominate a data protection officer** (DPO) for its local office. Appointing a DPO, publishing their contact details and providing them to the data protection authority are requirements for certain entities under the GDPR.[60] Relevantly for digital platforms, this includes entities whose core activities require large scale, regular and systematic monitoring of individuals (for example, online behaviour tracking).[61]

The Hamburg data protection authority, which imposed the fine, said 'This case should be a clear warning to all other companies: naming a data protection officer and telling the regulator about it are duties, which the data protection authority takes seriously. Even smaller violations like these can lead to substantial penalties.[62]

In a separate enforcement action, a German Court in May 2020 referred a case against Facebook to the European Court of Justice to seek clarification on the applicable law. The long-running case, brought by the Federation of German Consumer Organisations (vzbv), alleged that the social network had allowed operators of online games to improperly collect the personal data of people who played them.[63] In 2012, games on Facebook's App Center automatically signed users up to share personal data including their email address without asking for consent first. At the end of the game, users would see a message saying that the app could post their status, photos and other information.[64] Facebook has since changed its privacy settings, however such games, including quizzes, were previously widely used to harvest data about Facebook users.[65]

---

[59] Irish Data Protection Commission, *Annual Report 1 January 2019 – 31 December 2019*, p 42.

[60] UK Information Commissioner's Office, *Guide to the GDPR*.

[61] UK Information Commissioner's Office, *Guide to the GDPR*.

[62] See Stephanie Bodoni, 'Facebook's Tiny Privacy Fine Is a 'Warning,' Watchdog Says', *Bloomberg*, 13 February 2020.

[63] Douglas Busvine, 'Facebook German privacy case referred to European Court,' *Reuters*, 28 May 2020.

[64] Douglas Busvine, 'Facebook German privacy case referred to European Court,' *Reuters*, 28 May 2020.

[65] Douglas Busvine, 'Facebook German privacy case referred to European Court,' *Reuters*, 28 May 2020.

10.5.2 Ireland

The Irish DPC has opened eight inquiries into Facebook since the GDPR commenced operation in May 2018. Three of these related to aspects of Facebook's 2018 breach in which attackers were able to exploit a security vulnerability to gain access to personal data of 50 million Facebook users.[66]

The other five inquiries involved other aspects of GDPR compliance and are still open at the time of writing.[67] These included inquiries examining:[68]

- Compliance with **access and data portability obligations** including application of the right of access to personal data in the Facebook 'Hive' database and portability of 'observed' personal data
- The **legal basis for processing and transparency** in relation to Facebook's Terms of Service and Data Policy
- The **legal basis for processing in the context of targeted advertising** to users
- The **adequacy of security safeguards** following a security incident concerning storage in plain text of user passwords
- **Compliance with access obligations** following an access request for certain technical information.

The Irish DPC has also engaged proactively with Facebook outside of its formal inquiries. For example, it has taken a close interest in Facebook's plans to more tightly integrate with Instagram and WhatsApp. In January 2019, the DPC reported that it would be 'very closely scrutinising Facebook's plans as they develop, particularly insofar as they involve the sharing and merging of personal data between different Facebook companies.'[69] In another recent example, the DPC expressed displeasure at only finding out at the last moment that Facebook was planning to roll out a dating feature. The DPC raised concerns about the fact Facebook had failed to provide it with documentation in relation to any DPIA or decision-making processes undertaken in relation to the new feature.[70] Following the DPC's intervention, Facebook opted to postpone roll-out.

---

[66] See S Perez and Z Whittaker, 'Everything you need to know about Facebook's data breach affecting 50M users', TechCrunch, 29 September 2018.

[67] Irish Data Protection Commission, *2018-2020 Regulatory Activity under GDPR*, 23 June 2020.

[68] See Irish Data Protection Commission, *Annual Report 1 January 2019 – 31 December 2019*, pp 41-3.

[69] Irish Data Protection Commission, Statement on proposed integration of Facebook, WhatsApp and Instagram, 28 January 2019.

[70] See Irish Data Protection Commission, Statement on Facebook dating feature, 12 February 2020.

10.6 GDPR enforcement against Google

10.6.1 France

The French National Data Commission (CNIL) issued a €50 million fine to Google in January 2019 for **lack of transparency**, **inadequate information** and **lack of valid consent** regarding personal information collected for the purpose of ad personalisation.[71]

Regarding Google's lack of transparency, CNIL found that essential information about data processing purpose, the data storage periods, and the categories of personal data used for ad personalisation was excessively disseminated across documents and webpages.[72] It also found the information to be not always clear and comprehensive, with information about collection purpose described in a 'too generic and vague manner.'

CNIL also found that Google **violated its obligation to have a legal basis for processing personal information**. The GDPR contains six lawful bases for data processing, one of which is where the data controller has obtained the data subject's consent for processing. Google stated that it obtains the user's consent to process data for ads personalisation purposes and that this was its legal basis for processing. However, CNIL found that the consent is not validly obtained for two reasons**:** users' consent was not sufficiently informed and users consent was neither specific nor unambiguous.

Information to 'inform' users when giving consent was deficient. CNIL observed, for example, that Google's 'Ads Personalization' information did not make clear the plurality of services, websites and applications involved in these processing operations (Google search, YouTube, Google Home, Google Maps, Google Play Store, Google Photos…) and therefore of the amount of data processed and combined.[73]

Users could configure the display of personalised ads by clicking a 'More options' button and unticking boxes associated with ad personalisation. CNIL found that having the user select the 'More options' button and then un-tick options did not meet the 'unambiguous' component of consent. Under the GDPR, for consent to be unambiguous there must be a clear affirmative action from the individual. This standard cannot be met with pre-ticked selections.

Before creating an account, users had to tick the boxes « I agree to Google's Terms of Service» and « I agree to the processing of my information as described above and further explained in the Privacy Policy» in order to create the account. CNIL found that this approach bundled the consents to

---

[71] French National Data Protection Commission (CNIL), The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019.

[72] French National Data Protection Commission (CNIL), The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019.

[73] French National Data Protection Commission (CNIL), The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019.

different processing and therefore did not meet the 'specific' component of consent. CNIL observed that the GDPR provides that consent is 'specific' only if it is given distinctly for each purpose.[74]

10.6.2 Ireland

In 2019, the Irish DPC opened an 'own-volition' inquiry into Google. The inquiry concerns the legal basis for, and transparency of, Google's real time bidding and Google Authorised Buyers system. As part of its inquiry, the DPC is examining:[75]

- Whether Google has a **legal basis for processing personal data**, which may include special category data, via the Google Authorised Buyers mechanism.
- How Google fulfils its **transparency obligations** in relation to the processing of such personal data.
- Google's **data retention obligations** in the context of the Google Authorized Buyers Ad Exchange.

The Irish DPC has opened a second own-volition inquiry into Google to establish whether Google has a **valid legal basis for processing the location data** of its users and whether it meets its obligations as a data controller with regard to **transparency**.[76]

At the time of writing, both inquiries were ongoing.[77]

10.6.3 Sweden

In 2017, the Swedish data protection authority audited how Google handles requests from individuals to have search result listings that include their name removed from the search engine. In its decision the authority concluded that a number of search result listings should be removed and subsequently ordered Google to do so. In a follow up audit in 2018, the Swedish data protection authority found that Google did not properly remove two of the search result listings that the data protection authority had ordered it to remove in 2017. In one case Google interpreted what web addresses needed to be removed too narrowly. In the other case, Google failed to remove the search result listing without undue delay.[78]

The Swedish data protection authority also found that when Google removed a search result listing, it notified the website to which the link is directed in a way that gave the site-owner knowledge of which webpage link was removed and who was behind the delisting request. This allowed the site-owner to re-publish the webpage using a different URL, thus circumventing the delisting process.

---

[74] French National Data Protection Commission (CNIL), The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 January 2019.

[75] See Irish Data Protection Commission, *Annual Report 1 January 2019 – 31 December 2019*, p 43.

[76] Irish Data Protection Commission, *2018-2020 Regulatory Activity under GDPR*, 23 June 2020, p 33.

[77] See Irish Data Protection Commission, *2018-2020 Regulatory Activity under GDPR*, 23 June 2020, p 33.

[78] European Data Protection Board, 'The Swedish Data Protection Authority imposes administrative fine on Google', 11 March 2020.

The Swedish authority found that Google did not have a legal basis for informing site-owners when search result listings were removed and that Google was giving individuals misleading information in the request form. The authority ordered Google to cease and desist from this practice. It also issued a fine of €7 million.

10.7 GDPR enforcement against Twitter

10.7.1 Ireland

Since the GDPR took effect in May 2018, the Irish DPC has opened three inquiries into Twitter. Under those inquiries, the DPC is examining:[79]

- Compliance with **access and data portability obligations** including consideration of whether an access request was 'manifestly unfounded or excessive'
- **Obligations to implement organisational and technical measures to secure and safeguard personal data** following what the DPC considered to be a 'large number of breaches notified to the DPC during the period since 25 May 2018'
- Compliance with **breach notification obligations**, in particular, whether notification happened in a timely manner and whether Twitter documented the breach appropriately.

Twitter garnered attention in 2019 when it admitted that it had used user data for targeted advertising without consent.[80] It appears that the DPC's examination of Twitter's compliance with GDPR 'data protection by design' obligations and timing of breach notification (the second and third inquiries in the list about) were in consequence of this breach.

10.8 GDPR enforcement against WhatsApp

10.8.1 Ireland

The Irish DPC has opened two inquiries into WhatsApp which were ongoing at the time of writing but at a final stage.[81]

In the first matter, the DPC is examining WhatsApp's **lawful basis for processing** in relation to its Terms of Service and Privacy Policy. Specifically, the inquiry addresses the complainant's contention that processing in accordance with WhatsApp's Terms of Service was conducted on the basis of the data subject's **consent** but that that consent was not valid.[82]

In the second matter, the DPC is examining whether WhatsApp met its **transparency obligations** under the GDPR. In particular, the DPC is assessing the transparency of privacy information directed to both users and non-users of WhatsApp's services, including information provided to data subjects

---

[79] See Irish Data Protection Commission, *Annual Report 1 January 2019 – 31 December 2019*, p 41.

[80] See 'Twitter admits GDPR breach after exploiting user data', *Decision Marketing*, 8 August 2019.

[81] Irish Data Protection Commission, *2018-2020 Regulatory Activity under GDPR*, 23 June 2020, pp 34-5.

[82] See Irish Data Protection Commission, *Annual Report 1 January 2019 – 31 December 2019*, p 44.

about the sharing of information between WhatsApp and other Facebook companies.[83] The DPC has completed its investigation and, given the cross-border aspect of the inquiry, is currently consulting other EU data protection authorities before finalising the case.[84]

10.9 GDPR enforcement against other platforms

10.9.1 Germany

Berlin Commissioner for Data Protection and Freedom of Information (Berlin DPA) fined food delivery platform 'Delivery Hero' €195,407.[85] With the fine, the Berlin Data Protection Commissioner punished various individual GDPR breaches by the company. The majority concerned failure to respect the rights of data subjects, such as the **right to be informed**, the **right to have the data erased** and the **right to object**. The complainant, who expressly forbid the use of his data for advertising purposes, still received 15 advertising emails from the delivery service.[86]

10.9.2 Ireland

The Irish DPC has opened an inquiry into LinkedIn to examine LinkedIn's **legal basis for processing in context of targeted advertising to users**. This is a similar inquiry to those the DPC is conducting in relation to Apple and Facebook. The DPC opened each of the inquiries following complaints by French digital advocacy organisation, La Quadrature du Net. Issues that the DPC is specifically examining include whether consent and another legal basis can be relied upon jointly for processing.[87] The DPC is also examining the technological framework underpinning the analysis of users' behaviour and activities (including profiling) on the LinkedIn platform and how that relates to the delivery of targeted advertisements to the user.[88]

The DPC has also opened an inquiry into Instagram to examine Instagram's **legal basis for processing** and **transparency** in relation to its Terms of Use and Data Policy. The inquiry is examining whether Instagram made its legal basis for processing clear in privacy information for users. The complainant also alleges that Instagram's data processing was conducted on the basis of the data subject's consent but that that consent was not valid. The DPC has similar inquiries on foot with regard to Facebook and WhatsApp, all initiated by the same complainant – Austrian privacy advocacy organisation None Of Your Business.

Both are cross-border inquiries with the DPC required to consult relevant EU data protection authorities before finalising its investigation. At the time of writing, both inquiries were still open,

---

[83] See Irish Data Protection Commission, *Annual Report 1 January 2019 – 31 December 2019*, p 45.

[84] See Irish Data Protection Commission, *Annual Report 1 January 2019 – 31 December 2019*, p 45.

[85] Patrick Burkholder, 'Highest GDPR fine imposed in Germany', Digital Business News, 20 September 2019.

[86] Patrick Burkholder, 'Highest GDPR fine imposed in Germany', Digital Business News, 20 September 2019.

[87] See Irish Data Protection Commission, *Annual Report 1 January 2019 – 31 December 2019*, p 43.

[88] See Irish Data Protection Commission, *Annual Report 1 January 2019 – 31 December 2019*, p 43.

though the inquiry into Instagram was nearing completion with a draft report shared with relevant parties.[89]

The Irish DPC also initiated two own-volition inquiries. One into Tinder to 'establish whether the company has a **legal basis for the ongoing processing** of its users' personal data and whether it meets its obligations as a data controller with regard to transparency and its compliance with data subject right's requests.'[90] And another into Yelp and its compliance with Articles 5, 6, 7 and 17 of GDPR following a number of complaints about Yelp's website data processing practices.[91]

At the time of writing, those inquiries were ongoing.

10.9.3 Norway

The Norwegian Consumer Council has filed a GDPR complaint with the Norwegian Data Protection Authority about online dating platform Grindr, alleging the platform shares data including location and device information with more than a dozen companies for advertising purposes, in violation of GDPR requirements. Grindr offers social networking services to LGBTQ people, so sharing the fact that a user has the app installed on their device can give an indication of their sexual orientation.[92] Associating this information with an advertising ID then makes the user identifiable to third-party advertisers and across services, according to the report from the Norwegian Consumer Council.

10.10 Draft ePrivacy Regulation

The Privacy and Electronic Communications Directive (Directive 2002/58), otherwise known as the ePrivacy Directive, safeguards the confidentiality of electronic communications in the EU. The legislation is to 'complement and particularise' matters covered by the general data protection legislation in the EU. The Directive deals with a number of issues such as confidentiality of information, treatment of traffic data, spam and cookies. It was last updated in 2009 (Directive 2009/136). In this update, the Directive explicitly required consent from users to process their web cookies. This is why there are cookie consent popups on many websites.

Just as the Data Protection Directive has been replaced with the GDPR, there is a currently a draft ePrivacy Regulation in the works. The ePrivacy Regulations govern a specific subject area as compared to the GDPR, addressing in detail the confidentiality of electronic communications and the tracking of internet users. One significant reform is to expand the scope not only extraterritorially but to also cover a much larger class of communications. Significantly, this includes 'Over the Top' (OTT) communications which operate via internet services. The 2009 Directive update has led to an excess of cookie consent requests from websites. The new regulation aims to make it easier for browser settings to allow blanket acceptance or refusal of tracking cookies and other identifiers, and will clarify

---

[89] Irish Data Protection Commission, *2018-2020 Regulatory Activity under GDPR*, 23 June 2020, p 33.

[90] Irish Data Protection Commission, *2018-2020 Regulatory Activity under GDPR*, 23 June 2020, p 34.

[91] Irish Data Protection Commission, *2018-2020 Regulatory Activity under GDPR*, 23 June 2020, p 35.

[92] Jon Porter, 'Grindr shares personal data with ad companies in violation of GDPR, complaint alleges', *The Verge,* 14 January 2020.

that consent is not needed for non-privacy intrusive cookies aimed at improving our internet experience. Resembling the GDPR, the sanctions under this Regulation are just as tough.

The move from Directive to Regulation is to ensure uniformity in the enforcement of data protection rules. As seen above, the reforms are also to achieve the aim of extraterritoriality, which to an extent will force digital platforms to be more responsible and accountable for their privacy practices.

11. Hong Kong

In Hong Kong, the general rule is that, personal information obtained from digital platforms is regulated by the only personal data privacy legislation within the jurisdiction – the Personal Data (Privacy) Ordinance (PDPO) – which covers organisations in both the private and public sectors regardless of their size. Use of personal information must be consistent with or directly related to the original purpose for which the information is collected.

Under PDPO, it is not necessary for data users in Hong Kong to solicit consent from the individual before collecting their personal information (be it sensitive information or otherwise). The only legal requirement is that individuals be informed of the data collection. Consent only comes into play when there is a change in data use – Data Protection Principle 3 of the PDPO prohibits the use of personal data for any new purpose unrelated to the original purpose of collection, unless the secondary use is with the data subject's express and voluntary consent.

PDPO further requires that data users must obtain informed (explicit) consent before using a data subject's personal data for direct marketing or transferring the data to a third party for direct marketing.

11.1 Office of the Privacy Commissioner for Personal Data

The Office of the Privacy Commissioner for Personal Data (PCPD) is an independent statutory body set up to oversee the enforcement of the PDPO. Its duties include to investigate and resolve complaints and to provide legal assistance to victims whose privacy rights were infringed.

The PCPD has statutory power to conduct investigations of suspected breaches of the PDPO. If, upon investigation, it is found that a data user has contravened the PDPO, the PCPD may issue an enforcement notice directing remedial and/or preventive steps to be taken. Previously, only the contravention of an enforcement notice issued by the Commissioner was an offence. However, since 2012, contravention of certain provisions of PDPO also amounts to an offence.[93] Despite this, it is unlikely the PCPD will impose a severe penalty. The most severe penalties issued under the PDPO have resulted in fines of $2000 AUD or under.

11.2 Digital platforms subject to enforcement action

According to the PCPD's website, no digital platforms have been subject to privacy enforcement in the past. The closest thing to a regulatory action involved Facebook HK. After the Cambridge Analytica incident, PCPD launched an investigation into Facebook HK. However, upon investigation, it ruled that Facebook HK did not control the collection, storage, processing or use of data of its Hong Kong account holders, hence Facebook HK could not be regarded as 'data user' for the purposes of the PDPO.

[93] See PCPD, Table of criminal offences under the PDPO.

The PCPD contended that Facebook Ireland was the 'data user' of Facebook's Hong Kong account holders. Furthermore, the PCPD contended that no account holders in Hong Kong complained to the PCPD, hence no investigation was necessary.

In 2016, PCPD responded to a media enquiry on WhatsApp's Privacy Policy update – however, no enforcement actions were taken.[94]

Otherwise, the most prevalent type of enforcement actions of the PCPD are those against organisations who solicit business or donations through direct marketing means on digital platforms (via email, WhatsApp, and so on).[95] PCPD has also investigated the misuse of social network information for employment selection (in response to complaints being made) but this has never resulted in any enforcement actions.[96]

11.3 Data practices receiving regulatory attention

The PCPD has given attention to data practices connected to digital platforms. This has included giving attention to doxxing (researching and publicly broadcasting private or identifying information, especially personal information) and cyber-bullying. The PCPD strongly condemned 'despicable online weaponisation of personal data' on social media platforms, which exposes victims, particularly those performing public duties, to pressure and fear.[97] To address this issue, the PDPO was also recently amended to create a new offence in cases where a person discloses any personal data of a data subject without their consent (particularly a doxxing victim), and the disclosure causes psychological harm to the data subject including by intimidation.

PCPD seldom receives complaints or initiates regulatory actions for any kind of behavioural tracking, but the office is nonetheless concerned that organisations should be mindful of the privacy implications of profiling information obtained from social media.[98]

---

[94] PCPD, 'Privacy Commissioner Responses to Media Enquiry on the WhatsApp's Privacy Policy Update and the Vulnerabilities in iOS Software', 26 August 2016.

[95] PCPD, Presentation, Privacy and Social Media, 2018.

[96] PCPD, Presentation, Surprise minimisation – Social networks : Why privacy matters, 5 May 2014.

[97] PCPD, Media statement, Privacy Commissioner Condemns Doxxing Legislative Council Security Personnel, 10 May 2020.

[98] PCPD, Presentation, Surprise minimisation – Social networks : Why privacy matters, 5 May 2014.

12. India

India has only recently moved to regulate privacy. Introduction of a Personal Data Protection Bill follows the Supreme Court's decision recognising the existence of the right of privacy in India.[99] While the Bill imports a number of aspects of the GDPR into Indian law, some commentators have criticised how the Bill would regulate social media platforms, including provisions requiring user verification and giving too much scope to central government intervention in the operation of social networks.

12.1 Personal Data Protection Bill

The Indian Personal Data Protection Bill (PDPB) was introduced in December 2019. Inspired by the GDPR, it has been referred to as India's GDPR. Like the GDPR, the PDPB will apply extraterritoriality. This means that digital platforms that are not present in India will have to abide by the PDPB if they process personal data in connection with business carried out or the offering of goods and services to individuals in India or if they carry out any activity that involves the profiling individuals in India.

The rights under the PDBP are also similar to those in the GDPR and include the right to be forgotten. There is a difference in terminology with 'data subjects' under GDPR referred to as 'data principals' under PDPB and 'data controllers' known as 'data fiduciaries'. Moreover, the PDPB also emphasises the importance of protecting children's data by putting the obligation on data fiduciaries to not only obtain consent from a parent or legal guardian but to also verify a child's age before the processing of any personal data. Digital platforms may also be classified as 'guardian data fiduciaries' by regulations which means that they are barred from profiling, tracking or targeting advertising at children.[100]

The PDPB also includes the concept of social media intermediaries which is defined as a service that facilitates online interaction between two or more 'users' and allows users to disseminate media.[101] As such by this definition, digital platforms such as Facebook, Whatsapp and others will fall under this category. Certain social media intermediaries may be categorised as 'significant data fiduciaries,' which brings with it an obligation to provide users with an account verification mechanism.[102] The purpose of this provision is unclear. Commentators have highlighted that the fundamental issue here is that the obligation conflicts with a core tenet of similar legislation globally that has been emphasised in the Bill as well: data minimisation.[103] Arguably, the account verification mechanism will encourage

---

[99] See Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors.

[100] 'Draft data protection bill allows processing sans consent for security, credit scores, debt recovery', *The Economic Times*, 10 December 2019.

[101] 'Here's what social media firms require from draft Data protection Bill', Business Standard, 11 December 2019.

[102] T Rajwade and G Grover, 'India's Privacy Bill Will Alter How it Regulates Social Media Platforms, Not all of it Good', *The Wire,* 17 February 2020.

[103] T Rajwade and G Grover, 'India's Privacy Bill Will Alter How it Regulates Social Media Platforms, Not all of it Good', *The Wire,* 17 February 2020.

digital platforms that fall under this category to collect more information about their users than is necessary.

Notably as part of its enforcement mechanism, the PDPB has included an audit requirement where significant data fiduciaries must submit their processing to annual audit by independent auditors selected from a list approved by the data protection authority.

12.2 Information Technology Act

A year before the PDPB was tabled, the Indian government released a draft policy which seeks to amend India's Information Technology Act 2000. The Information Technology (Intermediaries Guideline (Amendment) Rules) 2018 was introduced with the aim to prevent spreading of fake news, curb obscene information on the internet, prevent misuse of social-media platforms and to provide security to users. [104]

The Rules specify that the intermediaries must inform users of the computer resource about the Rules and regulations and privacy policy so as not to host, display, upload, modify, publish, transmit, update or share any information which might affect public health and safety and Critical Information structure. Moreover, the intermediaries are also required to inform the user once a month about the fact that if the Rules and regulations, privacy policy and user agreement to access or usage of Intermediary computer resource are not complied with, then the intermediaries reserve the right to terminate such access and usage.

The draft amendment proposes that intermediaries are required to take down content deemed inappropriate by authorities. If a company receives a complaint from a law enforcement agency, the firm would be required to trace and report within 72 hours the origin of that content and to disable that user's access within 24 hours.

[104] Analysis of the Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018, *Lexology,* 27 March 2019.

13. Indonesia

In Indonesia, there is no general law on data protection. A new draft bill on the 'Protection of Private Personal Data' is currently under consideration by the Indonesian House of Representatives. If passed, the bill will become Indonesia's first comprehensive data privacy law.[105] The bill categorises violations against the data protection rules as criminal offenses and punishes intentional unlawful processing with up to seven years of imprisonment or punitive fines of up to 70 billion Indonesian Rupiah (IDR) (or approximately $7 million AUD). If the offender of the law is a corporation, the management or beneficiary owner can be held liable and face a prison sentence.

Currently, the primary sources of privacy law which regulate digital platforms or social media are: Law No. 11 of 2008 regarding Electronic Information and Transactions[106]; Law No. 19 of 2016 regarding the Amendment of Law No.11 of 2008[107]; Government Regulation No. 71 of 2019 (regarding Provisions of Electronic Systems and Transactions)[108]; and Minister of Communications & Informatics Regulation No. 20 of 2016 (regarding the Protection of Personal Data in an Electronic System).[109] Digital platforms fall under the definition of Electronic System Providers (ESP) under the Regulations.[110]

The Electronic Information Law stipulates that any use of personal data in electronic form must only occur with the consent of the individual.[111] A violation of this or other provisions may result in criminal penalties. The fines can go up to IDR 12 billion and the term of imprisonment ranges from 4 years to 12 years.

In 2016, the Indonesian Parliament introduced a right to be forgotten.[112]

13.1 Privacy regulator and powers

The key regulator for data protection in Indonesia is the Minister of Communications & Informatics (MOCI), whose task is to supervise the implementation of the above-mentioned regulations, particularly Law No. 11 of 2008 regarding Electronic Information and Transactions. Officials at the MOCI are authorised to request any data and information from an ESP to ensure its compliance with data protection rules.

---

[105] 'Indonesia to step up data protection with new bill amid booming digital economy', *Reuters,* 28 January 2020.

[106] Law No. 11 of 2008 regarding Electronic Information and Transactions.

[107] Law No. 19 of 2016 regarding the Amendment of Law No.11 of 2008.

[108] 'Indonesia: New regulation on Electronic System and Transactions', *Baker Mckenzie,* 28 October 2019.

[109] Minister of Communications & Informatics Regulation No. 20 of 2016 available at.

[110] 'Systems that function to prepare, collect, process, analyze, retain, display, publish, transmit and/or disseminate electronic information.' The MOCI has interpreted this to mean that any person or entity that stores data electronically is considered an ESP using an electronic system.

[111] Original wording: "Unless provided otherwise by Rules, use of any information through electronic media that involves personal data of a Person must be made with the consent of the Person concerned."

[112] 'Controversial 'right to be forgotten' finds its way into Indonesian law,' *TechInAsia,* 1 December 2016.

MOCI Regulation 20 Article 30 provides administrative sanctions in the form of verbal warnings, written warnings, temporary dismissal of activities and an announcement on MOCI's website stating that the party has not complied with data protection regulations. According to Article 36, the MOCI should coordinate with the Minister or Chief of Supervisory Agency to impose administrative sanctions against the relevant ESP.

In terms of legal reform, the Ministry of Communication and Information Technology (MCIT) is responsible for policymaking relating to information technology and communications.

13.2 Enforcement involving digital platforms

There has been minimal privacy enforcement of digital platforms in Indonesia. After the Cambridge Analytica incident, the National Police launched a criminal investigation into Facebook when it was revealed that more than 1 million Indonesian users were affected by the breach.[113]

Other enforcement involving digital platforms has tended to focus on problematic content. In 2020, Indonesian authorities blocked access to some Telegram channels, saying it had several forums that were 'full of radical and terrorist propaganda'.[114] In 2018, the Information Ministry issued a statement saying they decided to block the app after learning it contained 'pornography, inappropriate content and blasphemy.'[115] The MCIT is actively requiring digital media operators to conduct content filtering.[116] MCIT regulation No. 19 of 2014 on the Management of Internet Sites with Negative Content (Regulation 19/2014), stipulates that internet sites with 'negative content' as websites containing pornography and other illegal activities. The range of fines is being discussed within the ministry and will be around IDR 100 million to IDR 500 million ($9,000 to $42,000 AUD) per content item. If the platform does not comply, the government will prevent public access to the website.[117]

So far, the authorities have succeeded in getting social media companies Telegram and TikTok to establish content monitoring teams in Indonesia after briefly banning them over 'negative content.' Fines may be imposed in 2021.[118]

The MCIT contracted state-owned company PT Industri Telekomunikasi Indonesia to implement an internet censorship system aimed at identifying and blocking websites containing pornography and content deemed reprehensible. Following concerns that the government would use deep-packet inspection to identify the content, the ministry issued a statement to say the system would only conduct crawling.[119]

---

[113] 'Will Facebook Indonesia face criminal charges for data breach?', *The Jakarta Post,* 19 April 2018.

[114] 'Indonesia to lift ban on Telegram message service over security', *Reuters,* 1 August 2017.

[115] 'Indonesia blocks 'pornographic' Tik Tok app', *DW, 5 July 2018.*

[116] 'Indonesia to meet social media firms as it eyes 'negative content' fines,' *Reuters,* 6 November 2019.

[117] 'Indonesia will impose fines on Facebook and other social platforms due to negative content,' *KrAsia,* 4 November 2019.

[118] 'Indonesia to meet social media firms as it eyes 'negative content' fines,' *Reuters,* 6 November 2019.

[119] 'Indonesia's IT ministry announces purchase of IDR221 billion system to automate internet censorship,' *Coconuts Jakarta,* 9 October 2017.

14. Japan

Japan's reformed privacy legislation came into effect in May 2017 and is enforced by its new privacy regulator – the Personal Information Commission Japan.

14.1 Act on Protection of Personal Information

The Act on Protection of Personal Information (APPI) enshrined in law several core privacy concepts including purpose limitation, notice, access and correction. An amendment to the Act passed in June 2020 introduced a range of new provisions (reflecting trends in other jurisdictions) including:[120]

- Mandatory breach reporting
- Additional requirements related to pseudonymity
- Expanded individual rights including rights to object, to erasure and data portability
- Expanded extraterritorial operation of the APPI.

14.2 Guidelines on Digital Platforms

On 29 August 2019, the Japan Fair Trade Commission published draft 'Guidelines Concerning Abuse of a Superior Bargaining Position under the Antimonopoly Act on the Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc.' and released them for public comment. Following that consultation process, the Commission published a final version of the guidelines in December 2019.[121]

The guidelines clarify when collection of personal data can be considered an 'abuse of superior bargaining position' under the Antimonopoly Act and subject to an administrative fine. According to the guidelines, this includes acquiring personal information without stating the purpose of use to consumers and using personal information against the intention of consumers beyond the scope necessary to achieve the purpose of use.[122]

14.3 Transparency and Fairness Bill

On 28 February 2020, the Japanese Cabinet approved a bill on Improving Transparency and Fairness of Specified Digital Platforms ('Transparency and Fairness Bill'). The Bill creates an obligation for specified digital platforms to disclose certain information (including contract terms and conditions) and to notify users in advance of contract amendments. The Transparency and Fairness Bill also requires platforms to establish procedures and systems based on the principles prescribed by the Minister of

---

[120] See H Tanaka and N Kitayama, 'Japan's DPA proposes changes to APPI,' IAPP, 12 December 2019 and 'Japan enacts Amendments to the Act on the Protection of Personal Information,' IAPP 9 June 2020.

[121] Japan Fair Trade Commission, Release of the "Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc.", Press Release, 17 December 2019.

[122] J Amato and Y Kaiju, 'Japan's Antitrust Watchdog Prepares to Step Up Enforcement in the Digital Economy', *Winston and Strawn*, 11 February 2020.

Economy, Trade and Industry (METI). In addition, the Transparency and Fairness Bill establishes a system under which the METI may ask Japan's Fair Trade Commission to investigate platforms under the Antimonopoly Act where it identifies a possible violation of that Act.[123]

[123] T Dokei and H Nakajima, The Japan Cabinet proposed Direction of Bill for Digital Platform Transparency Act, White and Case, 8 January 2020.

15. New Zealand

The New Zealand Privacy Act has recently been reformed and the new Act is set to take effect from December 2020. The new Act introduces mandatory breach reporting, requiring organisations to notify both the regulator and affected individuals when there is a risk of serious harm arising from the breach.

Under the amended act, the Privacy Commissioner will have some new powers, including the ability to issue compliance notices to businesses or organisations 'to require them to do something, or stop doing something, in order to comply with the Privacy Act.'[124] Compliance notices will also state the steps that the organisation must take to remedy non-compliance with the Act and the date by which the organisation or business must make the necessary changes.[125] The amended Act also includes stronger information gathering powers.

In alignment with privacy law in other jurisdictions, the extraterritorial operation of the Privacy Act has been extended. The NZ OPC has specifically pointed out that its reformed Act will now apply to businesses located offshore like Google and Facebook.[126]

15.1 Engagement with digital platforms

Enforcement against digital platforms has been difficult in New Zealand due to uncertainty about the application of the New Zealand Privacy Act to organisations based offshore. For example, in 2018, the NZ OPC stated that Facebook had breached the New Zealand Act when it refused to process a person's access request.[127] Facebook stated, in response, that it was not covered by New Zealand's privacy legislation.[128] Reforms to the Privacy Act, described above, seek to remove that uncertainty and make clear that platforms like Facebook are covered and must comply.

In its 2018-19 annual report, the NZ OPC noted the importance of this extension of coverage, particularly in the context of Facebook's Cambridge Analytica scandal and social media platforms hosting disturbing videos of terrorist violence.[129] On the latter issue, the NZ OPC engaged in the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online – a cross-government and international initiative led by the New Zealand Government, following the 15 March 2019 mosque shootings in Christchurch. In connection with the Christchurch Call, the Privacy Commissioner expressed concerns regarding the ways social media companies collect and use

[124] NZ OPC, *Blog: Privacy 2.0: Key changes in the Privacy Act 2020*, 16 June 2020.

[125] NZ OPC, *Blog: Privacy 2.0: Key changes in the Privacy Act 2020*, 16 June 2020.

[126] NZ OPC, Privacy 2.0: Key changes in the Privacy Act 2020, 16 June 2020.

[127] NZ OPC, Press release, Privacy Commissioner: Facebook must comply with NZ Privacy Act, 28 March 2018.

[128] NZ OPC, Blog, Facebook: What this is really about, 3 April 2018.

[129] NZ OPC, 2018-19 Annual Report, p 2.

people's personal information and the algorithms digital platforms use to deliver personalised content to end users.[130]

Despite limited enforcement action up until now on digital platforms, the NZ OPC has been actively engaged in this space, using its platform to comment on and address privacy concerns, including in relation to: the Facebook Cambridge Analytica incident, sharing of data between What's App and Facebook, Google Street View collection of Wi-Fi data incident, Facebook's privacy settings and changes to Google's privacy policy.

[130] NZ OPC, 2018-19 Annual Report, p 16.

16. Singapore

The Personal Data Protection Act (PDPA) was enacted in 2012 and came into effect in 2014. The PDPA applies to the private sector (public agencies are exempt). It also has extraterritorial reach and explicitly applies to organisations who may not have any physical presence in Singapore. Thus, digital platforms must comply with the law. The enforcement authority in Singapore is the Personal Data Protection Commission (PDPC). The PDPC has produced additional sector-specific and industry guidelines, though no guideline has been produced for digital platforms.

The PDPC is authorised to give certain directions to organisations that have breached the PDPA. These include directions to:

- Stop collecting, using or disclosing personal data in contravention of the Act
- Destroy personal data collected in contravention of the Act
- Provide access to or correct the personal data and/or
- Pay a financial penalty of an amount not exceeding $1 million.

Recently the Singapore Ministry of Communications and Information and the PDPC announced a public consultation on a draft Personal Data Protection (Amendment) Bill. The key proposed amendments are:

- **Mandatory Data Breach Notification** – organisations must notify the PDPC of a data breach as soon as it is practicable (and in any case no later than 3 days after the day the organisation makes an assessment of a notifiable breach); as well as a requirement to notify affected individuals. The proposed parameters for notification are similar to the current best practice PDPC breach notification guidelines.
- **Wider Scope for Deemed Consent** – the concept of 'deemed consent' will be expanded in scope so as to also cover circumstances where: (i) the collection, use or disclosure of personal data is reasonably necessary to conclude or perform a contract or transaction; or (ii) where individuals have been notified of the purpose of the intended collection, use or disclosure of personal data, given a reasonable opportunity to opt-out, and have not opted out.
- **Data Portability** – individuals can request a copy of their personal data be transmitted to another organisation, enabling consumers to switch service providers more easily.
- **Higher Fines** – financial penalties for non-compliance with the PDPA will be increased up to 10% of annual turnover or S$1 million, whichever is higher.

The proposed introduction of a mandatory data breach notification and the increase of fines will strengthen accountability and push organisations to pay closer attention to data protection compliance. Singapore citizens were among those affected by the Cambridge Analytica case. However, at the time of writing no actions have been taken by the PDPC against Facebook.

17. United Kingdom

In 2018 the UK reformed its privacy law to align with GDPR requirements. (See section 10 for a more detailed discussion of GDPR.) The Data Protection Act 2018 (DPA 2018) is intended to be read alongside the GDPR, though the DPA 2018 covers aspects of the GDPR in more detail. It also contains protections about the role, functions and enforcement powers of the Information Commissioner's Office (ICO). Those enforcement powers have become stronger under the DPA 2018, and the ICO has issued a *Regulatory Action Policy* which sets out how the ICO 'will use [its] enhanced powers to pull back the curtain on processing where the public have concerns, for example social media companies, political parties, data brokers and the use of new technologies by law enforcement agencies.'[131]

The ICO also enforces the Privacy and Electronic Communications Regulations (PECR). The PECR regulates the sending of electronic marketing messages. It also requires organisations to provide information about the purposes of any cookie or similar technology that stores information (or accesses information stored) on user devices, and obtain prior consent.[132] The PECR sits alongside the DPA 2018 and the GDPR. The ICO has advised that the PECR (which predates the GDPR) is not replaced by the GDPR and that complying with PECR helps with complying with the GDPR, and vice versa – though there are some differences and organisations need to take care to comply with both.[133] For example, the PECR is not limited to applying to personal data.

At this point, the ICO has carried out formal enforcement against only one digital platform – Facebook. However, it is deeply engaged in a number of relevant areas of investigation including behavioural targeting for political purposes (see section 17.2) and privacy issues arising in connection with adtech (see section 17.3).

17.1 Enforcement against Facebook

The ICO fined Facebook £500,000 for serious breaches of data protection law in 2018. This was the highest fine it could impose under legislation now superseded by the DPA 2018. Under the GDPR, the fine would have been much higher. In parallel with investigations in other jurisdictions, the ICO found that 'between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' with people who had.[134]

The ICO also found that Facebook failed to keep the personal information secure because it did not properly oversee apps and developers using its platform. According to the ICO, '[t]hese failings meant one developer, Dr Aleksandr Kogan and his company GSR, harvested the Facebook data of up to 87

---

[131] UK Information Commissioner's Office, Annual Report 2018-19, p 23.

[132] See UK Information Commissioner's Office, Guide to PECR.

[133] See UK Information Commissioner's Office, Guide to PECR.

[134] UK Information Commissioner's Office, 'ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information', 25 October 2018.

million people worldwide, without their knowledge. A subset of this data was later shared with other organisations, including SCL Group, the parent company of Cambridge Analytica which was involved in political campaigning in the US.'[135]

17.2 Investigation of behavioural targeting and democracy

Following the Cambridge Analytica incident, the ICO investigated the use of analytics to target voters and published its findings in a report entitled 'Democracy disrupted: Personal information and political influence.' The report addressed changes to political advertising whereby political parties and campaign groups in the UK and beyond increasingly use personal information and sophisticated data analytics techniques to target voters.[136] The report sought to describe the role of key players in the digital political ecosystem including political parties, campaign groups, social media companies, data brokers and data analytics providers. On the whole, the ICO found serious deficits in transparency about the practices of these key players and made a number of recommendations for addressing privacy and ethical shortfalls.

In its 2018-19 annual report, the ICO noted that 'the investigation demonstrated the need for stronger guidance, as parties and campaign groups now increasingly use personal information and data analytics to target and influence voters.' The ICO is advocating for the guidance to be given statutory footing as a code of practice under the DPA 2018: '[w]e have called on Parliament to legislate to this end, and continue to do so.'[137]

17.3 Investigation of adtech and real-time bidding

The ICO has taken an active interest in privacy issues associated with the adtech industry and, in particular, the practice of real-time bidding (RTB). The ICO has sought to address the significant lack of transparency of RTB due to the nature of the supply chain and the many different actors and service providers that sit between the advertisers buying online advertising space, and the publishers selling it.[138] In June 2019, it published an 'update' report that outlined a range of issues and areas of possible non-compliance with DPA 2018.[139] The ICO set RTB against both the requirements of the GDPR and the PECR – particularly requirements related to transparency, lawful basis for processing and security.[140] The ICO found, in its update report, that:[141]

---

[135] UK Information Commissioner's Office, 'ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information', 25 October 2018.

[136] UK Information Commissioner's Office, *Democracy disrupted: Personal information and political influence*, 11 July 2018, p 3.

[137] UK Information Commissioner's Office, Annual Report 2018-19, p 22.

[138] UK Information Commissioner's Office, *Blog: Adtech - the reform of real time bidding has started and will continue*, 17 January 2020.

[139] See UK Information Commissioner's Office, Update report into adtech and real time bidding, 20 June 2019.

[140] See UK Information Commissioner's Office, Update report into adtech and real time bidding, 20 June 2019 p 15.

[141] See UK Information Commissioner's Office, Update report into adtech and real time bidding, 20 June 2019 p 23.

- Collection of both non-special category data and special category data was taking place unlawfully and should have been subject to consent.[142] Non-special category data was sometimes being collected on the basis of 'legitimate interest' (one of the six lawful bases under the GDPR) but ICO found that this was not appropriate grounds for placement and reading of cookies and other trackers on devices and, furthermore, adtechs needed to get consent anyway to comply with the PECR.
- Even if adtechs could rely on the 'legitimate interests' basis, they were unable to demonstrate that they had properly carried out the legitimate interests tests and implemented appropriate safeguards.
- There appeared to be low understanding of the data protection impact assessment requirement under GDPR and the ICO had low confidence that the risks associated with RTB had been fully assessed and mitigated.
- The privacy information provided to individuals was unclear and complex.
- There was inconsistent application of data protection by design requirements and little consideration of the limitations applying to international transfers of personal data.
- There were similar inconsistencies in application of data minimisation and retention controls.
- Individuals had no guarantee of the security of their information in the adtech ecosystem.

The ICO set out its next steps in the update report, which include further engagement with stakeholders, targeted information-gathering, cooperation with other data protection authorities and an industry sweep. In the meantime, the ICO stated that it 'expect[ed] data controllers in the adtech industry to re-evaluate their approach to privacy notices, use of personal data, and the lawful bases they apply within the RTB ecosystem.'[143]

Following engagement with key stakeholders in the sector, the ICO reports that Google has agreed to remove content categories and improve its process for auditing counterparties.[144] Google has also recently proposed improvements to its Chrome browser, including phasing out support for third party cookies within the next two years.[145]

---

[142] Under the GDPR, 'special category data' is similar to 'sensitive information' under the Australian Privacy Act 1988. It accrues some extra protections due to its sensitivity.

[143] See UK Information Commissioner's Office, Update report into adtech and real time bidding, 20 June 2019 p 24.

[144] UK Information Commissioner's Office, *Blog: Adtech - the reform of real time bidding has started and will continue*, 17 January 2020.

[145] UK Information Commissioner's Office, *Blog: Adtech - the reform of real time bidding has started and will continue*, 17 January 2020.

17.4 Code for age appropriate design

The UK ICO has developed an *Age appropriate design – a code for online services.*[146] The code is not yet in force and still subject to parliamentary approval. In its 2018-19 annual report, the ICO observed that '[a] key concept of the GDPR is that children merit special protection':

> This code will help to achieve that by setting out the standards of age-appropriate design which we expect providers of online services and apps to meet when their services are likely to be used by children or when they process children's personal data. This is a key example of how important and effective data protection by design can be.[147]

The code outlines 15 standards of age appropriate design with a focus on 'providing default settings which ensures that children have the best possible access to online services whilst minimising data collection and use, by default.'[148]

[146] UK Information Commissioner's Office, *Age appropriate design – a code for online services*.

[147] UK Information Commissioner's Office, Annual Report 2018-19, p 20.

[148] UK Information Commissioner's Office, *Age appropriate design – a code for online services*.

18. United States[149]

18.1 Federal Trade Commission

The US has traditionally taken a 'consumer protection' approach to overseeing privacy, as opposed to the more 'rights-based' approach in the EU. This has meant that the US has tended to pursue privacy issues through consumer protection laws rather than specific data protection legislation. The federal agency in charge of consumer privacy in the US is the Federal Trade Commission (FTC). Its primary legal authority comes from section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace.[150] This perhaps results in a greater emphasis on privacy notices, privacy policies and terms of service in that jurisdiction, with the FTC able to pursue an organisation for deceptive practices if the organisation acts contrary to its privacy policy.

Recently the FTC called on Congress to enact comprehensive privacy and data security legislation, enforceable by the FTC.[151] Following its recent settlement with Facebook (outlined below), three FTC Commissioners also suggested that '[t]he extent to which Facebook, or any other company, should be able to collect, use, aggregate, and monetize data, is something Congress should evaluate in its consideration of federal privacy legislation.[152] The Commissioners pointed out that their '100-year-old statute does not give us free rein to impose these restrictions.'[153]

The FTC is different from data protection authorities in other jurisdictions not only because it has a broader consumer protection remit, but also because it is a 'civil law enforcement agency' and not a 'regulator'.[154] It enforces the FTC Act via litigation or out-of-court settlement. FTC Commissioners have observed that, '[i]n order to serve the public interest and provide real protections for consumers, the Commission must compare settlement options against what it might reasonably obtain through litigation.'[155] This is of interest in the Facebook case where the FTC was able to reach a settlement with the company that imposed much higher penalty and more extensive 'conduct relief' than would likely have been available via litigation.

Reaching a settlement with an organisation commonly results in the FTC imposing an order on the organisation requiring it to do or cease certain actions and the order has the force of law when approved and signed by the district court judge.[156] Along with its enforcement action under the FTC

---

[149] California has recently enacted the California Consumer Privacy Act (CCPA) – legislation that introduces a new approach to data protection in the States. It has a number of features of interest from a 'digital platforms' standpoint and so is dealt with in a separate section – see section 8.

[150] FTC, *2019 Privacy and Data Security Update*, p 1.

[151] See FTC, Statement to the United States House of Representatives Committee on Appropriations, Subcommittee on Financial Services and General Government, 25 September 2019.

[152] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 6.

[153] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 6.

[154] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 6.

[155] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 6.

[156] See FTC, Press release 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook', 24 July 2019.

Act, the FTC also has enforcement oversight of a number of sector specific laws, along with the Children's Online Privacy Protection Act (COPPA) discussed below.[157]

18.2 FTC enforcement against Facebook

In 2019, the FTC imposed its largest penalty ever – $5 billion USD against Facebook. The FTC found that Facebook violated the Commission's 2012 order against the company by misrepresenting the control users had over their personal information and failing to institute and maintain a reasonable program to ensure consumers' privacy.[158] The FTC also alleged that Facebook deceptively failed to disclose that it would use phone numbers provided by users for two-factor authentication for targeted advertisements to those users.[159] Along with issuing a monetary penalty, the FTC amended the 2012 order to impose a number of new obligations on Facebook designed to change Facebook's overall approach to privacy.

This enforcement action offers an important case study for an investigation of regulatory responses to digital platforms. The amended order comprises a range of innovative and rigorous obligations for Facebook that, in many ways, go further than any other privacy enforcement action elsewhere in the world.

18.2.1 Alleged privacy violations

The FTC's original 2012 settlement with Facebook related to a finding that Facebook's practice of sharing a Facebook user's friends' data with third-party developers of apps was deceptive. From 2010, when a user downloaded a Facebook app, Facebook's default settings allowed the app developers to access information not only about the user but their Facebook friends as well. This meant that, unless a user changed settings on Facebook's 'Application' page (not the privacy settings page), their information could be shared with app developers even if it was their friend that downloaded the app and not them. The 2012 settlement imposed certain obligations on Facebook, including that it not misrepresent its privacy settings and data sharing practices and also that it implement a reasonable privacy program to safeguard privacy, confidentiality and integrity of user data.

In 2019, the FTC found that Facebook had breached the 2012 order and engaged in additional deceptive conduct. In particular, it was alleged that Facebook:[160]

- Removed information from its privacy page about its practice of sharing users' friends data with third party app developers

---

[157] Other sector-specific privacy related laws that FTC enforces include the Gramm-Leach-Bliley Act, the Truth in Lending Act, the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act.

[158] FTC, *2019 Privacy and Data Security Update*, p 2.

[159] FTC, *2019 Privacy and Data Security Update*, p 2.

[160] See Complaint for Civil Penalties, Injunction, and Other Relief, 24 June 2019, pp 3-6.

- Stated that it would stop app developers from collecting users' friends information but then continued to allow certain apps to collect this data
- Failed to vet third party developers before granting them access to consumer data and failed to fairly enforce its policies and terms and conditions against apps (particularly where there was a financial benefit to Facebook in not enforcing)
- Asked users to provide a phone number to enable two factor authentication and then failed to effectively disclose that phone numbers would also be used for advertising
- Implied to users that to use face recognition technology on Facebook they had to opt in when, in fact, they had to opt out to disable face recognition.

The complaint against Facebook pointed out that its core business model monetises user information by using it for advertising and argued that Facebook had subverted users' privacy choices to serve its own business interests.[161]

18.2.2 Obligations imposed on Facebook

The FTC's amended order imposed **general requirements** on Facebook including greater oversight of third-party apps, stronger data security, and clear and conspicuous notice of use of face recognition technology.[162] It also prohibited Facebook from using phone numbers, collected to enable two-factor authentication, for advertising.

The order also imposed major changes to Facebook's corporate governance which effectively removed CEO Mark Zuckerberg's unfettered control over decisions affecting user privacy.[163] In particular, the order included a number of **corporate governance requirements** and obliges Facebook to:

- Establish an independent privacy committee of Facebook's Board of Directors
- Designate compliance officers to be responsible for Facebook's privacy program; the compliance officers may only be removed by the Board privacy committee, not the Facebook CEO or Facebook employees
- Submit to the FTC quarterly certifications that the company is in compliance with the privacy program mandated by the order, and annual certification that the company is in overall compliance with the order
- Conduct a privacy review of every new or modified product, service, or practice before it is implemented, and document decisions about user privacy (and generate a quarterly privacy review report)
- Report privacy breaches involving 500 users or more to the FTC

---

[161] See Complaint for Civil Penalties, Injunction, and Other Relief, 24 June 2019, p 2.

[162] See FTC, Press release 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook', 24 July 2019.

[163] See FTC, Press release 'FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook', 24 July 2019.

- Submit to independent third-party assessment on a biennial basis to evaluate the effectiveness of Facebook's privacy program (the independent assessor must also report to the Board privacy committee every quarter).

FTC commissioners supporting the settlement noted that the order 'significantly diminishes Mr Zuckerberg's power—something no government agency, anywhere in the world, has thus far accomplished' and made it 'much harder for Mr Zuckerberg to steamroll the company into disregarding users' privacy, were that his goal, or claim plausible deniability about the company's privacy practices.'[164] This is because the order requires Zuckerberg to report quarterly – under threat of civil and criminal penalties – that the company's privacy program is in compliance with the order.

The corporate governance requirements multiply the layers of oversight and create a number of information channels to provide certainty that Facebook is meeting its privacy obligations. These include quarterly compliance certification; biennial independent assessments; quarterly reporting of the independent assessor to the Board privacy committee; quarterly reporting of privacy reviews; and breach reporting to the FTC. The FTC's intention has been to create 'an unprecedented level of transparency for Facebook's privacy practices.'[165]

18.2.3 Fine imposed on Facebook

The size of the penalty imposed on Facebook has garnered attention for obvious reasons. It is one of the largest civil penalties in US history – alongside only cases involving enormous environmental damage and massive financial fraud.[166] Five billion dollars was approximately 9% of Facebook's 2018 revenue, and approximately 23% of its 2018 profit.[167] In a statement about the case, FTC Commissioners Simons, Phillips and Wilson said: 'The magnitude of this penalty resets the baseline for privacy cases—including for any future violation by Facebook—and sends a strong message to every company in America that collects consumers' data: where the FTC has the authority to seek penalties, it will use that authority aggressively.'[168]

However, dissenting Commissioners objected to the size of the penalty, stating that, considering Facebook's revenue, it did not go far enough. Dissenting Commissioner Slaughter noted that 'as of [2019], Facebook brings in around $5 billion on a monthly basis.'[169] She also observed that '[t]he fact that Facebook's stock value increased with the disclosure of a potential $5 billion penalty may suggest that the market believes that a penalty at this level makes a violation profitable.'[170]

---

[164] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 7.

[165] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 3.

[166] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 2.

[167] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 1.

[168] See Statement of Chairman Simons and Commissioners Phillips and Wilson re Facebook. 24 July 2019, p 2.

[169] Dissenting Statement of Commissioner Rebecca Kelly Slaughter in the matter of Facebook, 24 July 2019, p 8.

[170] Dissenting Statement of Commissioner Rebecca Kelly Slaughter in the matter of Facebook, 24 July 2019, p 11.

18.3 FTC enforcement against Google

In 2012, the FTC imposed a $22.5 million civil penalty on Google related to charges that it misrepresented to users of Apple's Safari Internet browser that it would not place tracking cookies or serve targeted ads to those users.[171] The FTC charged that Google placed a certain advertising tracking cookie on the computers of Safari users even though Google had previously told these users they would automatically be opted out of such tracking, as a result of the default settings of the Safari browser used in Macs, iPhones and iPads.[172]

The penalty was at that time a record amount. Like the Facebook case, the FTC pursued Google on the grounds that it violated an earlier privacy settlement between the company and the FTC which barred Google from misrepresenting the extent to which consumers can exercise control over the collection of their information.

18.4 Children's Online Privacy Protection Act

COPPA is not new to the regulatory landscape in the States; however, it exerts considerable regulatory impact. Its drafters 20 years ago could not have predicted the extent to which digital platforms today would be driven by advertising revenue and the enormous power to be derived from harnessing personal information to deliver a 'personalised' user experience.

The Act regulates online collection of personal information of children – specifically those under 13. Although drafted many years before the GDPR, it follows the trend of extending the extraterritorial operation of domestic privacy legislation. The FTC has advised that COPPA applies to foreign-based websites or online services that are directed at children in the US or knowingly collect the personal information of children in the US.[173] It also applies to US-based companies that collect personal information of foreign children.[174]

COPPA and associated regulations requires website operators to:[175]

- **Include certain information in a privacy policy** about their information handling practices (as they relate to children's personal information)
- **Give a privacy notice** to parents before collecting their child's information
- **Obtain 'verifiable parental consent'** before collecting, using or disclosing personal information of children[176]

---

[171] FTC, Press release, 'Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser', 9 August 2012.

[172] FTC, Press release, 'Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser', 9 August 2012.

[173] FTC, Frequently Asked Questions, COPPA Enforcement, B7.

[174] FTC, Frequently Asked Questions, COPPA Enforcement, B7.

[175] See FTC, *COPPA: Six Step Compliance Plan for your Business*.

[176] See FTC, *COPPA: Six Step Compliance Plan for your Business*, Step 4.

- **Give parents a way to review the information held about their child**, revoke their consent and request that their child's information be deleted
- **Implement reasonable steps to protect security** of children's personal information and **delete children's personal information** when no longer needed for the purpose it was collected.

In 2013, the definition of personal information under COPPA was expanded to include:

- a persistent identifier that can be used to recognise a user over time and across different sites, including a cookie number, an IP address, a processor or device serial number, or a unique device identifier
- geolocation information sufficient to identify a street name and city or town.[177]

18.4.1 Enforcement action under COPPA

The largest settlement under COPPA to date was for $170 million USD in 2019. This was almost 30 times higher than the largest civil penalty previously imposed under COPPA.[178] The case involved YouTube. The FTC alleged that '…YouTube violated the COPPA Rule by collecting personal information—in the form of persistent identifiers that are used to track users across the Internet—from viewers of child-directed channels, without first notifying parents and getting their consent.'[179] The complaint to the FTC contended that YouTube earned millions of dollars by using cookies to deliver targeted ads to viewers of these channels.[180] In the words of FTC Commissioner Chopra, YouTube's violation was 'extremely serious': 'The company baited children using nursery rhymes, cartoons, and other kid-directed content on curated YouTube channels to feed its massively profitable behavioural advertising business.'[181]

The YouTube case is of interest to a study of regulation of digital platforms due to some novel elements, including its finding that:

- Individual channels on a general audience platform meet the definition of 'websites or online services' under COPPA – this indicates that the FTC considers content creators and channel owners to be standalone 'operators' under COPPA, liable for COPPA violations.
- The platform (in this case YouTube) has liability under COPPA as a third party. The FTC previously stated that platforms are not generally responsible for child-directed content that appears on them, unless the platform possesses actual knowledge that it is collecting personal

---

[177] See FTC, *COPPA: Six Step Compliance Plan for your Business*.

[178] See Statement of Joseph J. Simons & Christine S. Wilson Regarding FTC and People of the State of New York v. Google LLC and YouTube, LLC, September 4, 2019, p 1.

[179] FTC, Press Release: 'Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law', 4 September 2019.

[180] FTC, Press Release: 'Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law', 4 September 2019.

[181] Dissenting statement of Commissioner Rohit Chopra in the matter of Google and YouTube, 4 September 2019, p 1.

information from users of a child-directed site or service. The FTC specifically found that YouTube did possess 'actual knowledge'.[182]

Before the YouTube case, the largest settlement under COPPA was for $5.7 million USD in February 2019. It involved the social network TikTok (then known as Musical.ly). The FTC alleged that TikTok knew children were using the app but failed to seek parental consent before collecting names, email addresses, and other personal information from users under the age of 13.[183] Specifically, TikTok breached requirements to give notice, get verified parental consent and delete children's personal information on the request of parents.[184]

Prior to 2019, there were no COPPA settlements over $1 million USD. Given that enforcement powers under COPPA have not changed recently, this might indicate both a change in policy for FTC and the influence of other jurisdictions implementing higher penalties. However, some have criticised the COPPA penalties for being too low. Commentators pointed out that '[w]hile the $170 million fine may be a record for COPPA violations, Google's parent company, Alphabet, brought in $13 billion in revenue in 2018 [and] experts estimate [YouTube also] brought in $13 billion.'[185] In the YouTube case, dissenting FTC commissioner Chopra pointed out that '[t]he terms of the settlement were not even significant enough to make Google issue a warning to its investors.'[186]

Other enforcement action is on foot. For example, a coalition of consumer groups recently complained to the FTC about Amazon and its Echo Dot devices (a voice-activated digital assistant aimed at kids). The complaint alleges that the devices operate in breach of COPPA requirements.[187] Other complaints currently before the FTC concerning Amazon relate to Alexa and the privacy implications of 'always on' microphones.[188]

A summary of recent COPPA enforcement actions against digital platforms is given in the table below:[189]

Date	Digital platform	Settlement amount	Areas of non-compliance
Sept 2019	YouTube	$170 million USD	Failed to get parental consent

[182] See Statement of Joseph J. Simons & Christine S. Wilson Regarding FTC and People of the State of New York v. Google LLC and YouTube, LLC, September 4, 2019, p 1-2.

[183] FTC, Press Release: 'Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law', 27 February 2019.

[184] FTC, Press Release: 'Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law', 27 February 2019.

[185] Matt Binder, 'YouTube's $170 million fine isn't enough – and part of the FTC knows it', Mashable Australia, 5 September 2019.

[186] Dissenting statement of Commissioner Rohit Chopra in the matter of Google and YouTube, 4 September 2019, p 1.

[187] See Echo Kids Privacy.

[188] Adam Clark Estes, 'The terrible truth about Alexa,' *Gizmodo*, 29 April 2019.

[189] FTC, Legal Resources.

Date	Digital platform	Settlement amount	Areas of non-compliance
April 2019	i-Dressup.com (Unixiz inc)	$35,000 USD	Failed to get parental consent (i-Dressup.com sought parental consent but when a parent declined consent, it collected children's personal information anyway.) Failed to put in place reasonable security safeguards
Feb 2019	TikTok (previously Musical.ly)	$5.7 million USD	Failed to give notice Failed to get parental consent Failed to delete personal information on request
Feb 2018	Explore Talent (talent search company allowing users to find out about auditions, casting calls and other professional opportunities)	$235,000 USD	Inaccurate information in privacy policy Failed to give notice Failed to get parental consent
Jan 2018	VTech (toy manufacturer) and its Kid Connect app (that operated in conjunction with VTech toys)	$650,000 USD	Failed to give notice Failed to get parental consent Failed to put in place reasonable security safeguards.
June 2016	InMobi (advertising software used by apps to deliver location-based advertising, access to more than a billion devices)[190]	$950,000 USD	For apps directed at children: Failed to get parental consent (Also, deceptive conduct under the FTC Act).
Dec 2015	LAI systems and Retro Dreamer (app developers)	$360,000 USD	Developed apps directed at children: Allowed third party advertisers to collect children's personal information through the apps (including via persistent identifiers) Failed to comply with COPPA
Sept 2014	Yelp (online review platform)	$450,000 USD (Yelp)	Knew that under-13s registered for its app and failed to comply with COPPA in relation to those users

[190] Though InMobi is not strictly a digital platform, this case raises many of the same issues that arise in relation to digital platforms – namely, large market share (InMobi was collecting data from over a billion devices) and use of personal information for targeted advertising.

As highlighted in the table, the main reason for enforcement action was the failure of apps to get parental consent to collect and use children's personal information. This was often more broadly linked to a finding that the organisation knew it was collecting children's personal information and did not take steps to comply with COPPA. Recent cases also demonstrate the extraterritorial operation of COPPA with the InMobi, VTech and TikTok cases all involving respondent organisations outside the US.

18.4.2 Criticism of COPPA

Most criticism of COPPA centres around the difficulty of verifying age online. It can be difficult to do so without also impinging on privacy by having to collect personal information to enable verification. And many of the options for seeking parental consent allowed for under COPPA (parents signing a form and faxing it in, or calling a phone number, or connecting with trained personnel via video conference) are cumbersome and unworkable for many organisations. It leads to a situation where digital platforms like Facebook and others simply ban children under 13 from using their site rather than deal with the complexity of verifying age, seeking parental consent and dealing with children's personal information. Critics argue that this sends children to less desirable websites or encourages them to lie about their age. A study in 2011 revealed that nearly a fifth of the parents of 10-year-olds knew their child was on Facebook, as did a third of parents of 11-year-olds and more than half of parents of 12-year-olds. The study also found that 68 percent of parents of children under 13 on Facebook helped their child set up the account.[191]

The FTC is currently reviewing COPPA rules and assessing whether technological change necessitates changes to how COPPA operates in practice.[192]

18.5 Other privacy legislation under development

The **Privacy Score Act of 2020** is currently before Congress. If it passes, it would direct the FTC to issue privacy scores (a kind of risk rating similar to a Standard & Poor's credit risk rating) for certain interactive computer services. Customers could use the published score to assess the risk of engaging with a particular online service, for example, Google or Facebook.

A draft **Data Accountability and Transparency Act 2020** is also under development and would introduce a general ban on collecting, using, sharing personal data except for permissible purposes. The Act would also provide a general ban on the use of face recognition technology. Individuals would be given more rights over their data. More significantly, the Act allows individuals the right to challenge the reason for the collection of their data and request a human review of any automated decisions. The proposal involves the creation of a new independent agency dedicated to protecting individuals' privacy and implementing the Act. With regard to accountability, the proposal would require CEO certification of compliance with the Act and contains potential criminal and civil penalties

---

[191] Larry Magid, 'Unintended Consequences of FTC's New COPPA Children's Online Privacy Rules', Huffington Post, 8 April 2012.

[192] See FTC, Press Release, 'FTC Seeks Comments on Children's Online Privacy Protection Act Rule', 25 July 2019.

for CEOs and Boards. At this point, the proposal – developed by a Democratic senator – is unlikely to succeed in the Republican-controlled Senate.

A number of US states have moved to implement CCPA-like privacy laws. On 1 July 2020, Maine's Broadband Privacy Law will come into effect which focuses entirely on user data collected by Internet Service Providers. The law prohibits ISPs to use, disclose, sell or permit access to customer personal information unless the customer gives express, affirmative consent. Other states considering privacy bills include Nebraska, Virginia, Florida and New York. Earlier this year in March, lawmakers in Washington for the second year running failed to push through the Washington Privacy Act. The Act was influenced by the CCPA but if it does become law, it will likely surpass the CCPA as the most comprehensive privacy law in the US.

18.6 EU-US Privacy Shield Framework[193]

The EU-US Privacy Shield framework is designed to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU to the US. The Privacy Shield was established in 2016 as a replacement for the International Safe Harbor Privacy Principles, which the European Court of Justice declared invalid.

Like Safe Harbor, the Privacy Shield Framework is a voluntary self-certification scheme but with stronger and more detailed compliance obligations and more redress mechanisms. Some of the significant features of the Privacy Shield include:

- **Verification of compliance** – as part of the self-certification, the applicant must confirm how it has verified its compliance with the Privacy Shield – whether through in-house or third-party verification, and evidence of this verification must be provided when requested
- **Handling of sensitive information** – the Privacy Shield's definition of sensitive personal information equates to the EU definition. Privacy Shield companies must get opt-in consent before they can disclose sensitive information to third parties or use it for new purposes
- **Accountability for onward transfer** – a requirement that a third-party company processing data on behalf of a Privacy Shield-certified organisation must guarantee the same level of protection as the Privacy Shield company itself
- **Data integrity and purpose limitation** – a requirement that companies must delete personal data that no longer serves the purpose for which it was collected

The enforcement of the Privacy Shield is governed by EU privacy authorities and the FTC. Under the FTC Act, an organisation's failure to abide by commitments to comply with the Privacy Shield Principles may be challenged as deceptive by the FTC. The FTC has the power to prohibit such misrepresentations through administrative orders or by seeking court orders; violations of those administrative orders can lead to civil penalties.

---

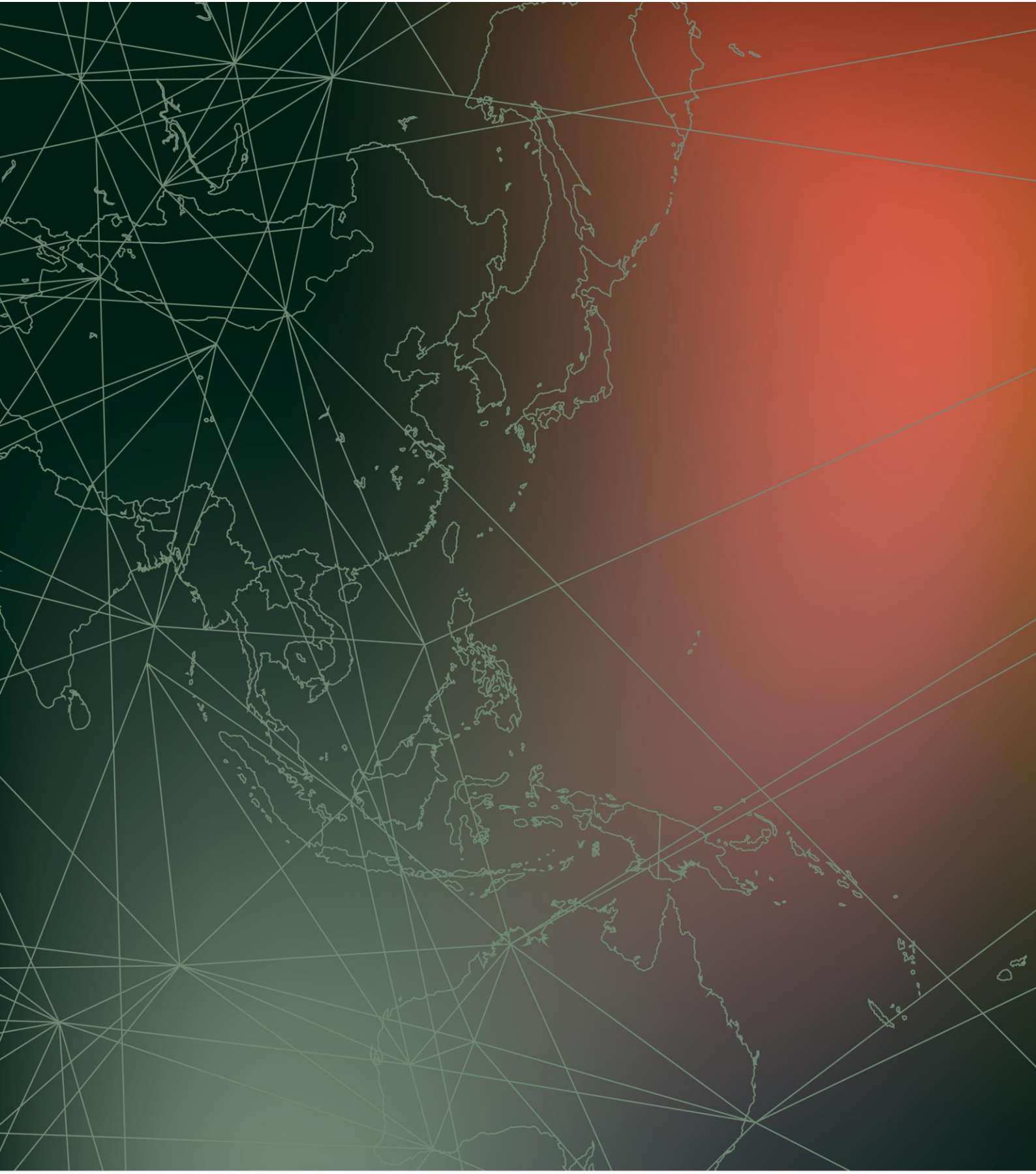
[193] Since the drafting of this paper, the European Court of Justice has struck down the Privacy Shield. On 16 July 2020, the Court held that personal data transferred to the US could not be protected in a way that satisfies requirements under EU law, particularly in regard to surveillance programmes carried out by the US and the lack of actionable rights granted to EU data subjects against US authorities.

In the past, the FTC has taken action against companies that falsely claimed certification under the Privacy Shield. However, most of these actions result in a settlement where the companies agree to halt misrepresentation and pay a fine. This does not provide a remedy to those whose data has been collected. As such, the FTC lacks effective enforcement authority.

19. Glossary

Acronym	Meaning
ACCC	Australian Competition and Consumer Commission
APEC	Asia Pacific Economic Cooperation
APPI	Japanese Act on the Protection of Personal Information
CalOPPA	California Online Privacy Protection Act
CBPR	APEC Cross Border Privacy Rules
CCPA	California Consumer Privacy Act
CNIL	French National Data Commission (France's data protection authority)
COPPA	Children's Online Privacy Protection Act (US)
CPRA	California Privacy Rights Act
DPA 2018	Data Protection Act 2018 (UK's main privacy law)
DPC	Irish Data Protection Commission
DPIA	Data Protection Impact Assessment
DPO	Data protection officer
ESP	Electronic System Providers (type of entity (which includes digital platforms) regulated by privacy related regulations in Indonesia
FTC	US Federal Trade Commission
GDPR	General Data Protection Regulation (the main privacy regulation in the EU)
ICO	UK Information Commissioner's Office
IIS	Information Integrity Solutions (privacy and security consultancy; authors of this paper)
MCIT	Indonesian Ministry of Communication and Information Technology
METI	Japanese Minister of Economy, Trade and Industry
MOCI	Indonesian Minister of Communications and Informatics
NZ OPC	New Zealand Office of the Privacy Commissioner
OAIC	Office of the Australian Information Commissioner
OPC	Office of the Privacy Commissioner of Canada

Acronym	Meaning
PCPD	Hong Kong Office of the Privacy Commissioner for Personal Data Protection
PDPA	Singapore Personal Data Protection Act
PDPB	Indian Personal Data Protection Bill
PDPC	Singapore Personal Data Protection Commission
PDPO	Hong Kong Personal Data (Privacy) Ordinance
PECR	Privacy and Electronic Communications Regulations (UK)
PIPEDA	Canadian Personal Information Protection and Electronic Documents Act
RTB	Real-Time Bidding (technique used by adtech industry when targeting ads to users)



INFORMATION
INTEGRITY
SOLUTIONS

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898