Into the iPhone: Smartphone Infrastructures, Internet and Data Law

Michael Veale[1,2]
[1]University College London
[2]University of Amsterdam

To appear in *Law, Policy and the Internet* (Lilian Edwards, Lachlan Urquhart and Catalina Goanta eds., Hart). Version May 12, 2026.

1 On Infrastructures

The internet was envisaged as a way to connect a world of different devices. The early design principles of the internet centred *openness* and *interoperability*—principles intended to ensure that no matter what kind of device you brought to the party, as long as you had a connection, you could take part in the fun without needing permission or a specific, proprietary bit of tech.[1] While this principle still holds true regarding a bare-bones connection to the network, people's experience of the internet is now much less about how you plug your device into it, now Wifi and mobile data are everywhere. It's more about what you can do when you are on the internet with the device that you are using.

1 Malte Ziewitz and Ian Brown, "A Prehistory of Internet Governance" in Ian Brown (ed), *Research Handbook on Governance of the Internet* (Edward Elgar Publishing 2013) DOI: 10.4337/9781849805049.

Devices matter to internet law for architectural reasons. The design of the internet makes it difficult to exert control from the network itself. Just because someone controls the telephone masts, cables or satellites, does not mean that they are able to meaningfully see, navigate or control the data flowing through this network. Even for the most powerful states with the most powerful intelligence apparatuses have been less and less able to snatch data from the middle of the network since Edward Snowden's leaks about US intelligence operations led to a massive uptake of the encrypted Web (the 'S' in HTTPS).

As the network has been a less important method of control, the most significant power in the modern internet has come from those who control the devices that are connected to it, and the platforms and services that people access from these devices.[2] In this chapter, we provide an introductory overview to some of the types of power and the legal issues that emerge from a focus on these devices, and indicate what those studying internet law might need to know to best think about this power.

2 Anticipating this possibility, see generally Jonathan L Zittrain, *The Future of the Internet and How to Stop It* (Yale University Press 2008); Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012) http://juliecohen.com/configuring-the-networked-self; on the political design of the internet, see generally Corinne Cath-Speth, "Changing Minds and Machines: A Case Study of Human Rights Advocacy in the Internet Engineering Task Force (IETF)" (DPhil, University of Oxford 2021) https://ora.ox.ac.uk/objects/uuid:9b844ffb-d5bb-4388-bb2f-305ddedb8939 accessed 6 September 2021.

Devices you connect to the internet with form part of a broader concept of *infrastructure*. The concept of infras-

tructure differs across academic fields. It is more of a way of thinking about technologies; a frame to use when it seems useful and appropriate to do so rather than a binary category into which technologies fall or do not fall. An infrastructure is something facilitative of other human activities, and typically enables the production of downstream goods and services.[3] Users of infrastructures often feel that they are generally *within them* rather than engaging with them explicitly and specifically, learning to take them for granted over time, and often only really noticing them when they break down and their real importance becomes apparent.[4] For example, people do not see that Amazon's cloud computing is such an important component of modern services until Amazon reports a widespread server outage and unexpected things in society stop working.

Infrastructures work in the background, but they do not typically work in a way we can think of as entirely neutral. They can advantage some actors over others, and create and exacerbate power relations between them. Some businesses have more power to access certain infrastructures than others, and some governments have more potential to reconfigure and intervene in them than others, given the characteristics of their jurisdiction or the economic levers they are able to pull. Some actors might be excluded from them entirely – think of a country or individual subject to US sanctions. All of these issues are important for studies of internet law and policy.

Infrastructures do not have to be some physically grouped or continuous thing like a data centre (although they can be). Infrastructures also exist in our pockets. In this chapter, we will look at pocket infrastructures. Through the lens of the *smartphone*, we will understand more about how infrastructures intersect with internet law issues, and how the law is perhaps starting to engage more directly with digital infrastructures than it used to. To ground us and provide a continuous case study, we will do this specifically through the lens of the Apple iPhone, a paradigmatic and in some ways quite extreme example of exerting power through device control.

We will first look at issues that come from how these devices constrain the kind of software that can run on them. From there, we look to state surveillance, how these infrastructures facilitate and resist being co-opted by states. We then look at corporate surveillance – a hybrid of the first two topics – to consider how infrastructures shape, enable and constrain the kind of behavioural analysis that is possible of individuals. Finally, we will look at how infrastructures such as the iPhone might facilitate information gathering and surveillance, by considering emerging issues in privacy-enhancing computation enabling such firms to analyse data without bringing it all together in one place.

3 Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) DOI: 10.1093/oso/9780190246693.001.0001 40.

4 Susan Leigh Star, "The Ethnography of Infrastructure" (1999) 43(3) American Behavioral Scientist 377 DOI: 10/b7hh4b.

2 There's No 'App' For That: Constraining software

When the internet was in its first few decades, especially from the late sixties onwards, individuals' devices typically ran programmes that those individuals actively chose to run, and which they could extensively customise and control. No single computer company had enormous sway, and the world had many very different, customisable devices that could run software programmes. Operating systems existed (and the market for them was fast consolidating around Microsoft Windows and Macintosh towards the end of that period) but they did not do too much to limit what people could do. Those firms instead favoured a strategy of encouraging a market of software developers to exist, largely to create as many new and exciting reasons as possible for people to purchase more of these strange 'personal computers'.[5]

Over time, business models relating to computers and the internet have changed drastically. This change culminated in the smartphone. The smartphone is without doubt the most commonly owned way for individuals on this planet to use the internet. With the smartphone, all software applications soon became just an 'app'. In a way, this was more than just a name change; it signified a new era of infrastructural power and control.

When the iPhone was released in 2007, there were no 'apps' on it as there are today. There was no App Store. Individuals could use a small handful of preinstalled software, including a calculator, a notepad, and a collaboratively-designed Google Maps service. They could also use websites, and they could save these websites to their homepages as 'web apps' (which had some limited ability to interface with the capabilities of the phone). They couldn't do much more. Indeed, one of the most bizarre things about the iPhone was just how limited it was compared to other devices at the time. Even if you wanted to, you couldn't build, buy, download or install any more software on it.

Even when the App Store launched the next year, this remained the same. No apps from any other sources could be installed. This set it apart from other smartphones and handheld devices – Apple had designed the operating system to severely restrict the capabilities of the user. In a world of eager hackers, this didn't last. In fact, it was only two weeks before hackers released a 'jailbreak' for the iPhone which bypassed the restrictions that Apple had placed, and allowed adventurous users to build and install their own custom software (albeit at serious risk of a voided warranty and a 'bricked' – a broken – device).

Over time, this power solidified. It became harder to 'jailbreak' and install custom applications on phones. Developers were forced to use the App Store to distribute software,

5 See generally on this period Laine Nooney, *The Apple II Age: How the Computer Became Personal* (The University of Chicago Press 2023).

and users were forced to go there to increase the functionality of their devices. All software had to pass the rules of the App Store – in 13 minutes per app, analysis in Cupertino decided what kind of apps were allowed, and which were not.[6] This meant that some types of software, despite technical feasibility, simply *could not be made* for Apple devices.

These rules and their implementation have been subject to a great deal of criticism. Some relates to very serious concerns. In late 2025, the US government contacted and pressured Apple to remove the 'ICEBlock' app from the App Store, designed to let people alert others about sightings of US immigration enforcers.[7] This followed conceptually similar police tracking apps being removed in Hong Kong in 2019.[8] Apple also acceded to government demands to remove VPN apps used to circumvent Web censorship in China, and to remove a tactical voting app produced by Alexei Navalny in Russia.[9]

While some apps are removed in relation to government pressure or based on controversial interpretations of Apple's own rules, others are not removed when they appear to seriously violate them. It took two years for Apple to take a more active stance on removing AI 'nudification' apps from the App Store, used to make non-consensual sexual imagery, as the firm refused to engage with the fact that while on the store itself, these apps were advertised as 'face swap' tools, they advertised their abusive potential widely across adverts on porn sites.[10] In 2026, as Grok, the AI tool attached to social media company X, was accused of unclothing and sexualising images of children upon request, Apple did not remove the app, and the UK government clarified that its intended prohibition on the distribution of nudification apps would not apply in this situation.[11] This was despite a similar situation in 2018 relating to Tumblr leading to the app's immediate, somewhat mysterious takedown, followed by an entire overhaul of its content moderation policies in an effort to be let back into the store.[12]

Furthermore, as Apple increased the functionality of iPhones with new sensors and capabilities, they designed the whole device so that not all apps could make use of these new features. Just because the hardware on an iPhone *could* do something in theory, does not mean an app could *make* it do it. Some features, such as the ability to 'tap to pay' using near-field communication (NFC), were only available to software that Apple made. Other features, such as Bluetooth, were only available in a limited, constrained way. This is done through limiting the availability or functionality of application programming interfaces, typically called APIs, which are ways that one piece of software, such as an app, can ask another, such as the operating system, to do something.

For example, even though iPhones had all the technical hardware needed to scan passports (requiring the same NFC technology used in contactless payments), Apple prohibited

6 Philip Shoemaker, "WWDC Preview With Apple's Former App Approval Chief" (*Bloomberg*, 28 May 2019) https://www.bloomberg.com/news/audio/2019-05-28/wwdc-preview-with-apple-s-former-app-approval-chief-podcast accessed 20 October 2025.

7 Tripp Mickle, "App That Tracks ICE Raids Sues U.S., Saying Officials Pressured Apple to Remove It" (*The New York Times*, 8 December 2025) https://www.nytimes.com/2025/12/08/business/apple-iceblock-lawsuit.html accessed 15 January 2026.

8 Jack Nicas, "Apple Removes App That Helps Hong Kong Protesters Track the Police" (*The New York Times*, 10 October 2019) https://www.nytimes.com/2019/10/09/technology/apple-hong-kong-app.html accessed 15 January 2026.

9 Andrew Roth, "Apple and Google Accused of 'Political Censorship' over Alexei Navalny App" (*The Guardian*, 17 September 2021) https://www.theguardian.com/world/2021/sep/17/apple-and-google-accused-of-political-censorship-over-alexei-navalny-app accessed 15 January 2026; "Apple 'Pulls 60 VPNs from China App Store'" (*BBC News*, 31 July 2017) https://www.bbc.co.uk/news/technology-40772375 accessed 15 January 2026.

10 Samantha Cole and Emanuel Maiberg, "A Popular Face Swap App Is Advertising Deepfakes on Porn Sites" (*VICE*, 10 May 2022) https://www.vice.com/en/article/face-swap-app-on-apple-app-store-google-play-deepfakes/ accessed 15 January 2026; Emanuel Maiberg, "Apple Removes Nonconsensual AI Nude Apps Following 404 Media Investigation" (*404 Media*, 26 April 2024) https://www.404media.co/apple-removes-nonconsensual-ai-nude-apps-following-404-media-investigation/ accessed 15 January 2026.

11 Mizy Clifton, "UK Nudification App Ban Won't Apply to Elon Musk's Grok" (*POLITICO*, 14 January 2026) https://www.politico.eu/article/uk-nudification-app-ban-wont-apply-to-elon-musks-grok/ accessed 15 January 2026.

12 Jason Silverstein, "Tumblr App Disappears from Apple's App Store Because of Child Porn" (20 November 2018) https://www.cbsnews.com/news/tumblr-app-disappears-from-apple-app-store-because-of-child-porn/ accessed 15 January 2026.

the UK government from using their 'private' (Apple-only) APIs in an app after the vote to leave the European Union to register EU citizens in the UK, despite ministers travelling to California on multiple occasions to grovel for this ability.[13] In the end, the UK government had to ask people to use their friends' Android devices, which were more permissive. Relatedly, in 2020, Apple refused repeated requests of ministers with responsibility for health in England and Wales to allow the government to use always-on Bluetooth for contact tracing purposes in a more invasive way that the manner they had proposed, leading to the eventual redesign of the contact tracing programme.[14]

On top of this, there is an array of infrastructural power that, often in the name of security, reduces the amount to which devices can be altered and repurposed. Much of this hails initially from the world of copyright and intellectual property. As computers and the internet made it easy to share and copy files and content, makers of content, software and hardware firms collaborated to solidify infrastructural power to limit users from doing so. Julie Cohen has called these arrangements 'architectures of control', and they have expanded in scope and reach in recent years.[15] When Netflix streams video to an iPhone, a user cannot take a screenshot or record the screen. This is not a simple voluntary instruction that Netflix gives; the video is played using a combination of encryption and Apple's 'secure enclave', a piece of hardware that is used to put a hard separation between some functions of the phone and others to create a guarantee that certain tampering or cross-contamination of code or information cannot happen. The section of the screen that is showing the decrypted video is isolated from the rest of the iPhone, meaning that it cannot be screenshotted or recorded by any app or process.[16] More and more apps and processes are using the secure enclave, from the storage of biometric readings to unlock your phone, to banking apps seeking extra security, to cryptographic functionality in the COVID-19 Bluetooth contact tracing apps used in the pandemic. There can be security benefits from the isolation and guarantees the secure enclave provides, but on the other hand, the technology cannot be scrutinised (because it is designed to not be examined or tampered with). The use of it does not just secure software against attackers, but it also can guarantee that functions of this software cannot be interoperated with or played with by other apps. The iPhone's on-device AI also makes use of the secure enclave, requiring it in order to access other files and services on the user's device, allowing, at the time of writing, Apple to hold a monopoly on on-device AI that can work across the messages, media and more stored on a user's phone.

13 See generally Caroline Nokes (then Minister of State for Immigration), House of Commons Home Affairs Committee, Tuesday 30 October 2018, 14.04pm. As insult to injury, Apple developed a way for developers to use this technology as the deadline for registering as an EU citizen in the UK passed. It is possible they did not want to have their brand associated with Brexit.

14 Michael Veale, "Sovereignty, Privacy and Contact Tracing Protocols" in Linnet Taylor and others (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020).

15 Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (n 1).

16 There is unfortunately no good academic explainer of this technology; it is called Apple FairPlay.

3 App law?

How should we understand 'apps' and their surrounding environment in relation to legal frameworks? As will be seen in the rest of this chapter, to do so requires a certain amount of legal eclecticism, as there is no single body of law that relates to 'apps' or software, let alone infrastructures, yet challenges we see emerging in one area have conceptual applicability across many, requiring internet lawyers to have solid familiarity across a large number of frameworks and regimes.[17]

It is worth noting that the power to constrain software held by Apple has been significantly amplified by the fact that Apple has, for a long time, resisted any calls to allow for alternative methods to distribute software for iPhones. In the UK, this is still the case. In the European Union, the Digital Markets Act now obliges the company to permit the installation of alternative app stores, which to some extent mitigates this issue.[18] It has also forbidden an operating system such as the iPhone's iOS to only give functionality to Apple applications or services.[19] These are unwieldy, underspecified provisions which have not generated, at the time of writing, notable or thriving alternatives, nor the awareness amongst European consumers that any alternatives exist. Apple has, furthermore, refused to de facto extend these rights jurisdictions such as China or the US, where we have seen some of the above controversies. Even European travellers to these jurisdictions find that their existing apps installed through a third-party app store cease updating after a month or so (a point we shall return to later). Europeans have had some functionality disabled (such as Wifi network sharing between Apple Watches and iPhones) so that Apple did not have to grant these permissions to third parties.

Some laws seek to ensure this infrastructural power to constrain software is wielded more responsibly. A new generation of platform liability law seeks to more deeply involve the state in the above decisions, as well as require some procedural fairness for developers whose software is disabled or removed. In the UK, the Online Safety Act plays this role. While it arguably already applies to app stores in relation to some of their functions, the government retained powers to make extensive secondary legislation to regulate the process of app store moderation, as well as giving itself extensive powers to make orders to app store to remove apps.[20] In the EU, the Digital Services Act would apply to moderation on app stores, and contains a variety of mechanisms to ensure that these processes are fairer.[21]

These two legal approaches – opening up, and making use of a bottleneck to govern – clash, which in turn reveals some of the core issues around infrastructural regulation. While the Digital Markets Act seeks to dilute infrastructural power, the Digital Services Act seeks to make use of this

17 See generally, as important early work on laws applicable to app stores, Daithí Mac Síthigh, "App Law Within: Rights and Regulation in the Smartphone Age" (2013) 21(2) International Journal of Law and Information Technology 154 DOI: 10.1093/ijlit/eat002.

18 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1 (DMA) art 6(4).

19 DMA, art 6(7).

20 Online Safety Act 2023, ss 146, 161, 215--6.

21 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC [2022] OJ L265/1 (DSA); see generally Martin Husovec, "Fair Moderation Process" in *Principles of the Digital Services Act* (Oxford University Press 2024) DOI: 10.1093/law-ocl/9780192882455.003.0011.

power to achieve policy aims, such as blocking or shaping the software market. In the United States, some have argued against alternative app stores precisely because of the lack of constitutional feasibility of creating a similar law to the Digital Services Act due to First Amendment free speech jurisprudence. They argue that the concentration of infrastructural power, and the privatised decision-making that results from it, is preferable to the governance vacuum in the US they expect would exist were these chokepoints to be weakened.[22] Others have argued that the assumption behind the Digital Services Act is that big actors have to stay big in order to remain powerful and wealthy enough to govern societal issues, causing significant problems of power imbalance in society and leading to today's digital oligopolies.[23]

Much of the infrastructure used to lock down and control devices is not just technologically protected, but has been legally protected too. Copyright owners, which can those writing the code for software, have the right under copyright law in the UK and many other parts of the world to use technological protection mechanisms (TPMs) – effectively, governance through code – to avoid unauthorised copying. Not only does the law give copyright users a right to do this, it holds liable, including criminally, entities that sell or distribute tools to tamper with these mechanisms.[24] The act of tampering is seen as the same as copyright infringement from a tort perspective, even if the individual may have had a legal route to copy the content they attempting to unlock to copy (because, for example, it was for parody or news reporting).[25] Such legal protections layered upon technical protections pose serious threats to what has been termed the "freedom to tinker", affecting both individuals and competing businesses seeking to understand, build and innovate upon an existing infrastructural base.[26]

4 Infrastructures and state surveillance

We now turn specifically to issues concerning the surveillance of individuals. Some of this concerns specific constraints on software and extends the discussion above, but in other areas, issues such as security and the facilitation of data collection and/or analysis play a larger role.

Devices are stores for much of the most sensitive data that people accumulate. They are the gateway for the majority of communications made by people over networks. They contain increasingly advanced sensors able to detect aspects of how they are used and the environments they are in. They also can leave traces and signals in our environments. These are signals that other sensors – and therefore other actors – can pick up and use for identification and tracking. Because of all the above, they are prime targets for those who wish to engage in surveillance, including corporations, govern-

22 Jane Bambauer and Anupam Chander, "Bills Meant to Check Big Tech' s Power Could Lead to More Disinformation" (*The Washington Post*, 6 June 2022) https://www.washingtonpost.com/outlook/2022/06/06/antitrust-bills-big-tech-hate-speech-disinformation/ accessed 15 January 2026.

23 Cory Doctorow, *How to Destroy Surveillance Capitalism* (Medium Editions 2021).

24 Copyright, Designs and Patents Act 1988 ss 296, 296ZB

25 Copyright, Designs and Patents Act 1988 s 296ZA

26 Pamela Samuelson, "Freedom to Tinker" (2016) 17(2) Theoretical Inquiries in Law 562 DOI: 10.1515/til-2016-0021.

ments, and even other individuals.

With this infrastructural capacity and power comes the responsibility to secure it against attackers. Hackers, such as those from state national security apparatuses, have long sought to turn phones into data mines, remote microphones, or location beacons. To do so, they seek 'zero-day exploits', bugs in an iPhone that Apple is wholly unaware of.[27] These exploits allow for the installation of spyware: software with heightened privileges on a device typically capable of exfiltrating data and executing commands. The GCHQ programme WARRIOR PRIDE centred on creating smartphone spyware that could retrieve files from iOS and Android devices, turn on the microphone at will, and geolocate victims, with each functionality given a different name of a 'Smurf' character, such as 'Nosey Smurf' for the microphone capabilities.[28] The Pegasus spyware was a later scandal. Pegasus is political explosive technology from Israeli software company NSO Group, a private firm selling surveillance technologies to governments which may not be able to set up extensive in-house development as GCHQ and the NSA can and have. The firm provided, effectively, state-level hacking-as-a-service. The Pegasus tool effectively allowed full, secret, real-time access to the functionality of someone's smartphone. It was widely used by repressive regimes around the world, including being associated with the murder of journalist Jamal Khassoggi by the Saudi Arabian state, and surveillance of political adversaries and civil society members.[29] Significant infrastructure providers require significant constant investment to protect users against such threats. In the cybersecurity space, being faced with a 'state-level actor' is commonly understood to be the hardest task to defend yourself against.

In situations where smartphone infrastructures successfully defend themselves and their users against state-level technical attacks, states might turn to the law instead. This enters a topic often called the 'crypto-wars', a term referring to law enforcement interests seeking legal remedies against technologists (in varying guises) to limit or compromise the use of encrypted communication. As communication, computer and encryption usage has become more complicated, so have the nature of these 'wars'.[30] Law enforcement often seeks to create 'back doors' into a secured system. This already sets up infrastructures for legal tensions – how to balance security and access. For example, European legal frameworks for smartphone security include obligations (in the relevant approved standard) to only weaken encrypted communication for reasons of interoperability, not law enforcement.[31] Many think such a balance is not possible, particularly as many adversaries are foreign governments, and to weaken in relation to some governments can create weaknesses others can exploit. As Apple's CEO, Tim Cook, said in 2015, "you can't have a back door that's only for the good guys".[32]

27 The name refers to the fact that when discovered, there will have been zero days for the security team to design or implement a fix.

28 James Ball, "Angry Birds and `Leaky' Phone Apps Targeted by NSA and GCHQ for User Data" (*The Guardian*, 28 January 2014) https://theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data accessed 3 May 2023.

29 See generally Laurent Richard and Sandrine Rigaud, *Pegasus: How a Spy in Your Pocket Threatens the End of Privacy, Dignity, and Democracy* (Henry Holt and Company 2023).

30 For a history of these, see Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (John Wiley & Sons, Incorporated 2020) s 26.2.7.

31 Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive [2022] L; *BS EN 18031-1:2024: Common Security Requirements for Radio Equipment - Internet Connected Radio Equipment* (British Standards Institute 2024) para 6.5.3 (a translated copy of a European Standard).

32 Robert Siegel, "Apple CEO Tim Cook: 'Privacy Is A Fundamental Human Right'" (*NPR*, 1 October 2015) https://www.npr.org/sections/alltechconsidered/2015/10/01/445026470/apple-ceo-tim-cook-privacy-is-a-fundamental-human-right accessed 16 January 2026; for scholarly analysis of the issue more generally, see Harold Abelson and others, "Keys under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications ‡" (2015) 1(1) Journal of Cybersecurity 69 DOI: 10.1093/cybsec/tyv009.

We see the clash of technical and legal methods when we look at the encryption of the files on smartphones themselves. Smartphones are typically encrypted so that individuals with physical possession of the phone cannot access its contents without the permission of the owner. Such encryption practices came to a head in 2015 when, after the San Bernadino shooting in the United States, the FBI sought support from Apple in decrypting a device – support which Apple did not provide.[33] The case was working its way to court, however the case was withdrawn after the FBI availed itself of the services of a private firm, almost certainly the Israeli firm Cellebrite, to crack the phone open.[34] This highlights an ongoing cat-and-mouse game, as these firms can often not unlock the very latest operating systems as Apple fortifies its infrastructure, but can compromise earlier ones from older or non-updated devices.[35]

To a degree that is yet to be fully tested, the US constitution gives American firms legal tools against some of these demands, creating challenges that internet lawyers should be aware of, as they have global repercussions. Governments requiring firms to make changes to their infrastructure would likely hit upon issues of 'compelled speech', which includes bespoke programming they are asked to do for policy ends, triggering the difficult test of 'strict scrutiny' under the First Amendment. This jurisprudence, developed in relation to religious speech, is increasingly playing a role in limiting the grip of US tech regulation or intervention, leading to challenges that the policy is not narrowly tailored enough for a compelling state interest, or that the state interest itself is insufficiently compelling.[36] Historically, the US regime has provided mixed blessings to the state of the regulation of infrastructural power throughout the world. On one hand, it has been political and legally difficult for both the US and non-US jurisdictions to direct the infrastructural designers at a company like Apple to do or not to do a certain thing, providing some level of shielding against meddling that international human rights law has not actively provided. Constitutional limitations on the 'speech' of firms like Apple might protect infrastructural change, assuming that firms take such legal battles, and are not pressured in other ways.[37] However, neither the US constitution nor its intelligence laws provide much in the way of rights or redress to foreigners who the US state wishes to learn about using the investigatory powers permitted within that constitutional framework. Most notably, this includes any information stored on US-affiliated cloud services which, as revealed by Edward Snowden, is examined for even mundane political surveillance.[38]

Some of this narrative is changing slightly, as both legal demands upon infrastructures, and growing demands for so-called 'digital sovereignty', are splintering technology regulation. While has long been the case, especially since the CJEU judgment in Google Spain which established the 'right

33 Karl Stephan, "Apple Versus the Feds: How a Smartphone Stymied the FBI" (2017) 6(2) IEEE Consumer Electronics Mag 103 DOI: 10/cwpf.

34 David Shamah, "Gov't Contract a Strong Sign FBI Used Israeli Tech to Crack San Bernardino iPhone" (*The Times of Israel*, 4 April 2016) http://www.timesofisrael.com/fbi-contract-a-strong-sign-fbi-used-israeli-tech-to-crack-san-bernardino-iphone/ accessed 16 January 2026.

35 Joseph Cox, "Leaked Docs Show What Phones Cellebrite Can (and Can't) Unlock" (*404 Media*, 17 July 2024) https://www.404media.co/leaked-docs-show-what-phones-cellebrite-can-and-cant-unlock/ accessed 16 January 2026.

36 Rebecca Aviel and others, "From Gods to Google" (2025) 134 Yale Law Journal 1269 DOI: 10.2139/ssrn.4742179.

37 Alan Z Rozenshtein, "Surveillance Intermediaries" (2018) 70 Stanford Law Review 99.

38 Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others" *The Guardian* (7 June 2013) https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data accessed 24 June 2025; See some of the legal consequences of this in *Big Brother Watch and Others v the United Kingdom* App no 58170/13, 62322/14 and 24960/15 (ECtHR (Grand Chamber), 25 May 2021) (relating to the PRISM system).

to be forgotten from search engines in the EU,[39] that *services* delivered across the world differed, for example in what they provided and what they blocked, we are seeing a growing willingness for firms to provide different infrastructures, such as smartphone operating system functions, depending on where users are located.

In the surveillance space, this splintering of surveillance and infrastructural governance is playing out in many fora. One follows the UK demand, under the powers in the Investigatory Powers Act 2016, to require Apple to redesign their 'Advanced Data Protection' system to allow law enforcement access. This system is a way that smartphone infrastructures can be designed to hold and manage keys and data such that cloud services and backups, such as for photos, videos, messages and even documents, are inaccessible even to Apple, known as end-to-end encrypted storage. It responds to the PRISM programme revealed in the Snowden leaks, which found that companies could be easily ordered under US law to provide access to encrypted files held by cloud companies.[40] It is also common knowledge that this remained (and often still remains) the weak point of many encrypted messenger services, as while such services encrypted the messages between two recipients, one individual of them might be making an unencrypted backup of their device which contains all the messages, and this backup could be obtained by a requesting state, or obtained through hacking into their accounts. Until the launch of the (optional) Advanced Data Protection scheme, the data in Apple's iCloud service could be accessed by Apple, and thus vulnerable to a warrant.[41] Advanced Data Protection, when enabled, meant that it was not.

In 2025, a secret order was made by the UK Home Secretary to Apple, requiring the firm, under a 'technical capability notice', to compromise the design of its system to enhance law enforcement access.[42] The existence of this notice was leaked, likely by Apple itself as a method to lobby against the decision, to the Washington Post.[43] The post was likely chosen as a non-UK newspaper that could cover such issues more freely without risk of the type of extreme reporting injunctions possible in the UK when national security issues are involved.[44] Legal action relating to this is ongoing,[45] but the issue notably became more political when the Trump Administration took a stance on it, with Director of National Intelligence Tulsi Gabbard pointing to the risks that this request, given its jurisdictional scope, would have on *Americans*.[46] The UK government stood down this request, but it is unclear at the time of writing whether they have altered the jurisdictional scope and reapplied for it.

Relatedly, the UK Government has codified an unprecedented legal power in relation to smartphone infrastructures, security and privacy. The Investigatory Powers Act contains, as of a 2024 amendment, a pre-notification requirement which applies to operating system providers of

39 Case C-136/17 *Google Spain v AEPD and Mario Costeja González* ECLI:EU:C:2014:317.

40 50 U.S.C. §1881a

41 Mike Isaac, "Apple Still Holds the Keys to Its Cloud Service, but Reluctantly" *The New York Times* (21 February 2016) https://www.nytimes.com/2016/02/22/technology/apple-still-holds-the-keys-to-its-cloud-service-but-reluctantly.html accessed 24 June 2025.

42 Investigatory Powers Act 2016 s 253

43 Joseph Menn, "U.K. Orders Apple to Let It Spy on Users' Encrypted Accounts" *The Washington Post* (7 February 2025) https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/ accessed 25 June 2025.

44 See eg *Ministry of Defence v Global Media and Entertainment Limited & Ors* [2025] EWHC 1806 (Admin), (relating to the data breach behind the Afghan Relocations and Assistance Policy).

45 Bernard Keenan, "Apple's Appeal to the Investigatory Powers Tribunal over the UK's Encryption 'Backdoor' Explained" (*Computer Weekly*, 2 April 2025) https://www.computerweekly.com/opinion/Apples-appeal-to-the-Investigatory-Powers-Tribunal-over-the-UKs-encryption-back-door-explained accessed 24 June 2025.

46 Tulsi Gabbard, "Letter to Senator Ron Wyden and Representative Andy Biggs" (*Office of the Director of National Intelligence*, 25 February 2025) https://perma.cc/2GRH-56SP.

smartphones. This requires such providers, including Apple, to notify the Secretary of State in relation to any changes to their device which might affect their ability to provide data in response to a warrant.[47] Introduction of encryption onto messaging services, for example, would have to be notified. The idea here is that it is easier to stop something than it is to undo it after it has been implemented. While the structure of the law does not technically require the Secretary of State's approval, they can, after receiving notice, issue a an order to prevent or alter this change under different legal powers, making it a de facto gatekeeping obligation.[48]

47 Investigatory Powers Act s 258A.

48 Investigatory Powers Act, s 253 (`technical capability notices').

5 Jurisdiction and sovereignty

Such orders to change or alter infrastructures for surveillance or other purposes have global effects in practice, even if they do not necessarily require it in law. Even were an order to draw narrow jurisdictional boundaries, such boundaries have to function technically, and they typically do not so do well or robustly. This is the benefit of governing through code compared to the messy jurisdictional question that often plague internet law – in practice, 'the jurisdiction [..] is the network itself'[49] – but this also can serve as its drawback when there are many clashing laws and ideals. This is because infrastructures shape features and services that sit atop of them, rather than are delivered immediately, transiently and transactionally at a given moment.

49 Joel R Reidenberg, "Lex Informatica: The Formulation of Information Policy Rules through Technology" (1998) 76(3) Texas Law Review 553, 570.

Some infrastructural laws' jurisdictional scope functions based on where a user is at a given moment of use. European roaming rules, which cap wholesale and retail mobile telephony costs, are an example of this. Users step into or out of different regimes and can have their billing calculated, whether they are a user or a resident.[50] However, a user cannot step in and out of infrastructures such as end-to-end encryption so easily without breaking them. For example, imagine a regime that removes encrypted protection on new data created depending on the jurisdiction a user is currently in. Such a regime opens up the possibility of an attack possible anywhere in the world, including outside of the jurisdiction that made the order, by 'fooling' a user's device to think they are in a different jurisdiction to the one they currently are in. Similarly, challenges emerge when people communicate across jurisdiction, such as when someone from a regulated jurisdiction is added to a group chat in a non-regulated jurisdiction. Laws that are introduced where encrypted storage is already present, insofar as they require decryption of already-encrypted data, run into challenges around how this can be done, as by definition the provider has very limited ability to decrypt end-to-end encrypted data without user co-operation.[51]

50 Regulation (EU) 2022/612 of the European Parliament and of the Council of 6 April 2022 on roaming on public mobile communications networks within the Union [2022] OJ L115/1 (Roaming Regulation).

51 Where the provider can control the operating system and the private key is held on device for convenience, it may be possible to roll out an operating system update that automatically uploads the private key to the server for decryption.

Much depends on whether the provision reduces security, as the above would, or if it is about the provision or non-

provision of an optional, separate service. Apple currently enforce the Digital Markets Act, mentioned earlier, in a manner related to the location of the user, switching them into the European regulatory system after a certain number of days – meaning they can install apps from outside of the App Store – and out after another number of days.[52] As the regulation is silent on how to manage this type of transition, this is an issue that may play out in the courts.

Some obligations to regulate infrastructure also work on the basis of where a device in the infrastructure was *sold*, rather than where the user is. This means that while devices look the same on their face, they may differ in terms of the underlying technology and functionality, creating a two-tier governance system that affects users regardless of where they move. For example, iPhones sold in mainland China run similar services to those in other parts of the world, but the cloud servers are operated in a joint venture with a company from data centres in Guizhou, chosen by the company in a botched effort to win favour with a promising local official they thought may succeed Premier Xi Jinping. It is unclear, and matter of constant factual dispute, as to the extent to which Chinese user data is available to the Chinese authorities.[53] Such governance steps around the issue of changing servers and standards, but in turn requires import controls in order to segment the regulated infrastructure in the market from the non-regulated infrastructure on sale outside of it.

The situation as it stands is that laws relating to surveillance and infrastructure rarely try to limit the jurisdictions that they affect, even if their orders only require certain jurisdictional results in order to consider any obligations discharged. The result of this can be clashes, and general unworkability, especially in the areas of national security where sovereignty issues are often at the fore. Such laws attempt to alter infrastructures in the name of security, but that precise same type of alteration happening externally can threaten the same security of these states. The dynamic of how this plays out across the world in a world of shared infrastrucutre is, therefore, very important.

States could try an resolve these tricky issues through international agreements – the US referred to a potential breach of the CLOUD Act restrictions on mutual surveillance of US and UK citizens when it engaged in a political to-and-fro regarding the Apple Advanced Data Protection System.[54] Yet these agreements are not only difficult to agree but difficult to monitor and enforce if they are agreed.

Instead, a core emerging reaction has been for governments to seek greater national control of digital infrastructures, potentially reducing the heavy interdependence and allowing more independent action. The smartphone market, a duopoly of two operating systems in the West, will be daunting to splinter meaningfully. The only real exception so far is to be found in China. Huawei's HarmonyOS

52 They also have to have their device as registered for purchases in the EU, which is quite a complex process and sometimes requires a national method of payment.

53 Patrick McGee, *Apple in China: The Capture of the World's Greatest Company* (Simon & Schuster 2025) ch 32.

54 Gabbard (n 4).

operating system, with its version 5 launched in late 2024, is truly distinct from Android and iOS, although unavailable elsewhere in the world at the time of writing.

6 Infrastructure and corporate surveillance

We now turn from state surveillance to consider surveillance more widely. Devices both contain sensitive data and are ways to access and target individuals for commercial purposes. It is therefore no surprise they are incredibly desirable for corporate surveillance.

There are so many apps in the world. The locked down nature of iOS makes studying them, including their surveillance practices, very difficult for scholars or regulators to do.[55] Data protection regulators have demonstrated limited capacity to regulate all the software in the world, and therefore it is questionable to what extent the law functions as a deterrent to invasive tracking practices by firms.[56] The result of this is that the enforcement vacuum has been somewhat filled, at least in part, by the private governance provided by the app store and the smartphone infrastructural ecosystem more broadly, as discussed above.

Data protection law does not explicitly place obligations on app stores or smartphone infrastructures, instead focussing on the concept of the data controller, the actor who determines the means and purposes of processing.[57] In a classic understanding of European law, an app store is an intermediary and an app is a controller. Unlike much internet law, which tries to go after chokepoints in a network in order to not have so many entities to regulate directly,[58] data protection law is structured as to only be able to go after entities that themselves have a hand in the data processing in question. This has been a core tension in the law, expanding the notion of controllership to many 'joint controllers', some of which have an infrastructural role, meaning that while European data protection law does not consider intermediaries as within its scope definitionally, it can try to incorporate those category of actors as the direct actors to be regulated.[59]

A core question is to what extent smartphone infrastructures should have responsibilities for the content they facilitate. Scholars have already documented the roles they are taking in the privacy space, and these roles are gaining in scope and complexity over time.[60] Given the visibility over the code submitted to Apple and the functions of the phone being requested, the App Store is an important potential gatekeeper here. The App Review guidelines replicate some of the higher level principles of data protection law, including purpose limitation and data minimisation in relation to data collection inside the app. In 2023 – 4, Apple claims to have rejected 375,000 apps from the App Store on privacy grounds.[61]

55 See generally Konrad Kollnig, "Regulatory Technologies for the Study of Data and Platform Power in the App Economy" (DPhil, University of Oxford 2023) https://ora.ox.ac.uk/objects/uuid:b6a86de2-37be-4c00-817d-34171454d5bf accessed 8 November 2024.

56 Konrad Kollnig and others, "Before and after GDPR: Tracking in Mobile Apps" (2021) 10(4) Internet Policy Review DOI: 10.14763/2021.4.1611.

57 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 (GDPR) art 4(7); Ronan O Fathaigh and Joris van Hoboken, "European Regulation of Smartphone Ecosystems" (2019) 5(4) European Data Protection Law Review (EDPL) 476 DOI: 10/ghm8qm.

58 Jack L Goldsmith and Tim Wu, *Who Controls the Internet? Illusions of a Borderless World* (Oxford University Press 2006); Ian Brown and Christopher T Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press 2013); Natasha Tusikov, *Chokepoints: Global Private Regulation on the Internet* (University of California Press 2016).

59 Case C-49/17 *FashionID* ECLI:EU:C:2019:629; Case C - 210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388; and in the most direct manner yet, Case C-492/23 *Russmedia* ECLI:EU:C:2025:935.

60 Joris van Hoboken and R Ó Fathaigh, "Smartphone Platforms as Privacy Regulators" (2021) 41 Computer Law & Security Review 105557 DOI: 10.1016/j.clsr.2021.105557.

61 Apple, "App Store Stopped over $7 Billion in Potentially Fraudulent Transactions" (*Apple Newsroom*, 14 May 2024) https://www.apple.com/newsroom/2024/05/app-store-stopped-over-7-billion-usd-in-potentially-fraudulent-transactions/ accessed 16 January 2026.

We also see that the Apple operating system has built in restrictions which serve regulatory functions. In order to use sensors capable of more invasive data collection, the app has to make a request to the operating system for the sensor via an API. A deep part of the operating system called the kernel checks each of these requests to see whether the app has permission to do so. Some permissions need to be granted by Apple itself as an 'entitlement' at the point of review to qualify for App Store listings. Others (also) require user consent, which cannot be done in a way that the app designs or chooses, and cannot be skipped or hidden, but requires the use of operating system designed boxes which are prominent and intrusive. These are not signals that the app can choose to disregard. If the consent from these boxes is not given, the app cannot complete the activity, as the smartphone infrastructure forbids that data or command flow to happen.

The smartphone infrastructure also facilitates law in other ways, forcing transparency and accessibility of legal requirements. For example, unless a qualitative purpose is given to the user when certain invasive sensors, the camera, the microphone and similar are requested to be used, the consent boxes are designed to crash the app immediately.[62] In doing so, this functions as an accountability mechanism that can trigger data protection law obligations, important as granular purposes for data processing are often missing from data controllers' information to data subjects.. Apps similarly have to link to an existing privacy policy with certain features to be permitted onto the App Store, making it visible to regulators and users.

In the words of Tania Bucher, an API can be an 'object of intense feeling' among developers and other interested parties.[63] The most intense feelings around Apple's privacy practices in relation to third party developers have centred around the ATT (App Tracking Transparency) system. Apps used to be able to use an API to request the unique, permanent ID of a user's phone without permission, which would allow them to link a user across different installed apps to connect behavioural tracking data. After a million of such records leaked alongside usernames, zip codes and more, claimed to be stolen from an FBI laptop by a hacking group, Apple phased these out for an identifier that could be reset by the user through a deeply hidden setting in the system options.[64] In 2021, Apple introduced ATT, removing the previous identifier, and requiring users to say yes to each app they want to permit to link their tracking data to data collected in other apps on their device, and giving an option for users to turn off apps' ability to ask them.

These infrastructural changes led to the advertising industry projecting massive losses. While there was a likely significant economic impact on some firms, the industry was not left in tatters as some predicted. Data analysis indicates that few firms exited the market, and instead they generally

62 See eg Apple, "Requesting Authorization to Capture and Save Media" (*Apple Developer Documentation*) https://developer.apple.com/documentation/AVFoundation/requesting-authorization-to-capture-and-save-media accessed 16 January 2026.

63 Tania Bucher, "Objects of Intense Feeling: The Case of the Twitter API" (2013) 3 Computational Culture: A Journal of Software Studies http://computationalculture.net/objects-of-intense-feeling-the-case-of-the-twitter-api/ accessed 17 June 2019.

64 Chris Soghoian, "Apple's Persistent Device ID Is a Threat to Privacy" (*American Civil Liberties Union*, 4 September 2012) https://www.aclu.org/news/national-security/apples-persistent-device-id-threat-privacy accessed 16 January 2026; Jessica E Vascellaro, "Apple to Release New Tracking Tool for App Developers" (*Wall Street Journal*, 8 June 2012) https://www.wsj.com/articles/SB10001424052702303665904577454653752815434 accessed 16 January 2026.

adapted to the changed environment.[65]

Competition authorities have been active in taking cases against this infrastructural change. Given that apps are broadly non-compliant with data protection law, and enforcement of this law is lacking, ATT has been somewhat effective in mitigating some of the most egregious harm from illegal data collection, even though ATT did not emanate directly from a legal requirement.[66] Competition authorities however argue that apps have to gain two sets of consent in order to track users now – the Apple technical consent via ATT, then a set with legal characteristics, and try to draw a comparison between the consent flow for third party apps and other consent flows in the iOS infrastructure, although these are often little strained given they have different purpose than tracking across apps. This, they argue, unacceptably advantages Apple, or acts as a barrier to competition. This area is one of deep tension. Some argue that data protection is in general used as a shield to prevent competition law enforcement.[67] Others see ATT as a valuable contribution to adding human rights constraints to a *de facto* unregulated market that competition authorities should step back from.[68] Scholars note that it still leaves large room for tracking even when consent is refused – room that firms are still making use of.[69] The advertising industry was livid – the head of the major industry body confusing commentators by calling those concerned about privacy in the sector 'extremists'.[70]

This is all made more confusing by the fact that data protection law, including recent and proposed amendments in the UK and the EU, places *more*, not less, emphasis on using browsers and operating systems to send signals to ask apps not to track. UK law now states explicitly that the signifying of consent in the context of tracking such as cookies may happen through the "amending or setting controls on the internet browser which the subscriber or user uses" or "using another application or programme", the implication being that such consent is not given in the context of tailored, persuasive messaging provided by an app, yet is valid regardless.[71] The European Union, at the time of writing, is proposing an 'Omnibus' reform of data protection law which has related provisions. This follows the broad history of 'do not track' obligations, which typically failed due a lack of agreed standardisation that the industry would respect, and lack of specificity in the laws that reference them.[72]

All in all, we see smartphone infrastructures as highly contested sites of privacy regulation, subject to legal claims from multiple direction in relation to their exercising of power in this space. To what extent we move to regulate *through* them more, or attempt to prevent them from regulating entities that rely on them in the name of the free market, is yet to be seen.

65 Cristobal Cheyre and others, "Did Apple' s App Tracking Transparency Framework Harm the App Ecosystem?" [2023] CESifo Working Paper No 10456 DOI: 10.2139/ssrn.4467977.

66 Konrad Kollnig and others, "Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels" (FAccT '22, Association for Computing Machinery 20 June 2022) DOI: 10.1145/3531146.3533116 516.

67 Giuseppe Colangelo, "The Privacy/Antitrust Curse: Insights from GDPR Application in Competition Law Proceedings" (2025) 70(1) The Antitrust Bulletin 113 DOI: 10.1177/0003603X241283975.

68 Alan Butler and Cali Schroeder, "Let' s Not Get Competitive About Tracking Mobile Users: How EU Competition Authorities Are Threatening to Roll Back Privacy Protections on iOS" (*EPIC - Electronic Privacy Information Center*, 22 October 2025) https://epic.org/lets-not-get-competitive-about-tracking-mobile-users-how-eu-competition-authorities-are-threatening-to-roll-back-privacy-protections-on-ios/ accessed 16 January 2026.

69 Kollnig and others (n 6).

70 Butler and Schroeder (n 6).

71 Data (Use and Access) Act 2025, sch 12; amending Privacy and Electronic Communications Regulations 2003.

72 Irene Kamara and Eleni Kosta, "Do Not Track Initiatives: Regaining the Lost User Control" (2016) 6(4) International Data Privacy Law 276 DOI: 10/gdxwds.

7 Facilitation of data analysis and information asymmetries

Lastly, smartphone infrastructures can facilitate data analysis and collection in more sophisticated ways than websites, services or apps. These methods are becoming increasingly important.

Contemporary software engineering relies heavily on a methodology called 'agile' development to proceed. This relies on constant feedback on how users use a software, and frequent updates being delivered to the software, such that users are in a situation of 'perpetual beta', with the infrastructure and its capabilities shifting all the time.[73] This contrasts to users subjected to the staggered release familiar from the days when people bought occasionally bought the latest version of software in oversized boxes from shops.[74] AI development builds on this, taking constant feedback from humans in order to tweak, detect errors and generally improve models for their next versions.

73 Seda Gürses and Joris van Hoboken, "Privacy after the Agile Turn" in Evan Selinger, Jules Polonetsky, and Omer Tene (eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018) DOI: 10.1017/9781316831960.032.

74 Yes, this actually happened!

Smartphone infrastructures could facilitate the collection of plenty of data and pass it to the entity that builds the system. Some do, at least at times. But as mentioned, these devices record some of our most sensitive experiences, and data flows from them to a firm like Apple *en masse* would attract consumer attention and regulatory ire. Unlike the relative free-for-all of the app markets described above, smartphone manufacturers are easy, rich targets for data regulators, and collection of too much data would lead to a liability timebomb.

This is one of the main reasons why smartphones are at the frontier of technology deployment in a field varyingly known as 'privacy engineering', 'privacy-enhancing technologies' or 'confidential computing'. These technologies seek to enable the completion of tasks, learning about the world, or the training of models, without transferring any more data about identifiable individuals than *needs* to be transferred.

That need, it turns out, can be quite low if you have enough control of big, networked groups of computers – like smartphones. A range of technologies, many deeply mathematical and statistical, exist which allow an infrastructure to do things that you might assume would need a lot of transfer and centralisation of sensitive data.

Consider the keyboard. Keyboards on tiny little touchscreens work because they are predictive, and try to work out what you wanted to type, rather than what you precisely, physically did. This requires a lot of learning about different types of people and the ways their hands write and type, and styles across languages and dialects. It also requires a lot of information about vocabulary. If you are someone who types a lot of niche words, or names from your contacts, your phone will be personalised to that. But the global model –

the model shipped to all phones, and regularly updated – needs to learn about the new vocabulary and styles that are emerging over time, else people would experience constant cycles of personal frustration as the world changed, as well as a long period of adjustment and training (both for them and their device) every time they got a new phone.

This kind of learning could happen through the central collection of a large amount of data, but consider for a moment how risky that would be. How would the device know what was bland and safe to send, and what was sensitive and could disclose private things about the people involved? Messengers that were end-to-end encrypted, or files that were being typed in and designed to be confidential, could no longer make those privacy and security guarantees when the data from the keyboard itself was leaving the device. What would stop a password, or banking 'memorable information' from being sent? After all, this is why cybercriminals often use 'key-loggers', either malicious spyware or actual physical, tampered-with keyboards people break into organisations to install, in order to exfiltrate the information being entered onto them.

Instead, keyboards on smartphones, including iPhones, use technologies such as *federated learning* to improve keyboards as a whole. This is a form of machine learning where a model can be updated in lots of little fragments from lots of different sources. It can be made to preserve the confidentiality of data used to create these fragments with statistical safeguards, such as a large amount of added noise, which make it difficult or impossible (depending on who you ask) to work out centrally what was being typed on any one phone. The noise added to each individuals' contribution to the updated model is so extreme it is designed to make each users' contribution look like nonsense, but at the enormous scale that Apple runs at, the noise gives way to a signal about the way in which typing and language is changing.

These technologies sit alongside a wide variety of others. Consider, for example, Apple's 'Iconic Scenes'. This technology, running in the background of every modern iPhone, sees Apple assemble a central database of what kind of photos people take where, in order to choose the right album covers for people's 'memories'. It is done through an incredibly technically involved pipeline – photos are tagged with an on-device neural network as to what is in them, and then some noise is added to the location and the description of the photo. Apple receives these noisy image descriptions and from the aggregation of all the noisy image descriptions, works out which are the images people like to take, and where, so they can show apt and salient photos to people.

While these two examples seem fairly innocuous, they imply that infrastructures have the ability to expand greatly (especially in light of the detailed sensors they have) to learn a huge amount about the world. With great knowledge may

come great power, and the need to constrain that power. Consider if a firm with infrastructural power like Apple's decided to learn about the location of all the LGBT venues in a city, by using on-device analysis of people's search history and user profiles, and people's common geolocation patterns on their mapping apps. It would be totally plausible to produce a list of where people who are, based on on-device analysis, assumed to be LGBT, hang out in groups, and if these groups were large enough, it can be argued this is information about the city, or the environment, not personal data relating to a single person. But put this technology in a repressive regime, and you can see that the value of non-personal data or knowledge is not ethically neutral, but, especially when derived and aggregated from personal information, comes with important questions about who gathers it, how, and for what purposes.[75]

There are quite detailed legal questions here, which this chapter cannot hope to do more than highlight. To what extent is data protection triggered here, given that the central organisation does not itself hold personal data about individuals, but instead such data stays on users devices? This is a complex question, because the law does not anticipate situations where no data controller has access to the data, and so even if the law does apply due to its wide scope, it does not always make a lot of sense.[76] To what extent can individuals opt-out of this? Possibly, using rights in the e-Privacy Directive, but these are quite blunt and broad, referring to anything stored on or retrieved from a terminal device. If this avenue is explored to deeply, given the wide text of the law, we may find there are very few things that would not require consent online.[77]

Infrastructures fundamentally challenge our understanding of data collection and analysis, which commonly focusses on words like collect, accumulate, access, or similar.[78] None of those verbs are needed here, as infrastructures compute over data whilst *leaving it where it is*. Infrastructure is effectively a substitute for data amalgamation. Regulators have already encountered versions of these issues through technologies such as Google's proposed 'Privacy Sandbox', which saw attempts (largely shot down for now by competition authorities) to abolish third-party cookies on websites, and instead store data about people's behavioural habits on their devices, and learn about them in a distributed way using some of the technologies described above.[79] Such technologies continue with profiling and manipulation, but may fix some issues of confidentiality. In general, infrastructures for surveillance and data processing will force us to more thoroughly ask – what (if anything) do we feel is wrong about behavioural analysis and interventions once such analysis and interventions happen in total confidence?

These issues become increasingly important as AI systems are sold by entities like Apple, which integrate with on-device data (through technologies called retrieval-

75 Michael Veale, "Rights for Those Who Unwillingly, Unknowingly and Unidentifiably Compute!" in Hans-W Micklitz and Giuseppe Vettori (eds), *The Future of the Person* (Hart Publishing 2025) DOI: 10.5040/9781509982752.

76 Michael Veale, "Denied by Design? Data Access Rights in Encrypted Infrastructures" (*SocArxiv*, 27 July 2023) DOI: 10.31235/osf.io/94y6r.

77 Veale, "Rights for Those Who Unwillingly, Unknowingly and Unidentifiably Compute!" (n 7); on the breadth of these provisions, see Lilian Edwards, "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective" (2016) 2(28) European Data Protection Law Review 28 DOI: 10/gdxwf5.

78 Michael Veale, "Some Commonly Held but Shaky Assumptions about Data, Privacy and Power" in Maria Ioannidou and Despoina Mantzari (eds), *Research Handbook on Data, Privacy and Competition Law* (Edward Elgar Publishing 2025) DOI: 10/qm9r.

79 Lee McGuigan and others, "The After Party: Cynical Resignation in Adtech's Pivot to Privacy" (2023) 10(2) Big Data & Society DOI: 10.1177/20539517231203665; Michael Veale, "Confidentiality Washing in Online Advertising" in Corinne Cath-Speth (ed), *Eaten by the Internet* (Meatspace Press 2023) DOI: 10.31235/osf.io/53ays.

augmented generation and semantic indices) to allow people to analyse, reason about and connect everything together, across apps and services. How will these systems improve, and who will benefit from such improvement? As always, an underlying issue in technology law is *cui bono* – who benefits?

8 Concluding remarks

In this chapter, we have attempted to give an introduction to how smartphone infrastructures interplay with issues of internet law. The breadth of this topic means no single section can be as deep or comprehensive as we might wish. There are many more questions we have not covered, and some may not yet have been considered at all. One thing we know is that infrastructures such as smartphone devices are crucial to the governance of the modern internet and are a site of regular contestation.

Even as this chapter has been finalised, there are growing discussions of areas that could not be included, such as client-side scanning – the technology that may require operating systems to scan for illegal content, such as child sexual abuse material, or to scan content sent or viewed by minors to prevent inappropriate material reaching them. There are also prominent discussions about intimate partner abuse, much of which is entangled with questions of tracking using mobile devices and infrastructures like Apple's Find My network, or the generation of AI-altered images for intimate image abuse using models that can run on people's devices.

All of the issues discussed here require some synthesis of technical understanding with legal creativity. A lot of the time, our contemporary ways of talking about technologies and data are challenged by infrastructure, which requires us to think in ways that may be unfamiliar or to use analogies we would not first turn to. The law, too, is often written with particular technical and economic arrangements in mind, and not all of these hold true as technologies change (even if there were ambitions to write the laws in a 'technology-neutral' manner). Infrastructural power is hard to characterise or summarise. By their very nature, infrastructures facilitate some forms of activity and constrain others. This means we have to be open to analysing them in an equally fluid way. Creating a vocabulary for discussing them will be crucial for the internet lawyers of the future.