the global voice of
the legal profession®

Government Access to IT Systems

By the IBA's Legal Practice Division
22 September 2019

Task Force Chairs

Erik Valgaeren *Technology Law Committee, Stibbe, Brussels, Belgium*

Sylvia Khatcherian *Technology Law Committee, Past Chair of Legal Practice Division, New York, USA*

Task Force Members

Steve Crown *Human Rights Institute, Microsoft, Washington, USA*

Johan Kahn *IP Committee, Kahn Pedersen, Stockholm, Sweden*

Souichirou Kozuka *Space Law Committee, Gakushuin University, Tokyo, Japan*

Laurent De Muyter *Communications Law Committee, Jones Day, Brussels, Belgium*

Jana Pattynova *Communications Law Committee, Pierstone, Prague, Czech Republic*

Julian Hamblin *Technology Law Committee, Womble Bond Dickinson, London, UK*

Research Support

Allison Holmes *Kent Law School, Kent, UK*

Contents

Introduction

Data is becoming the core asset of our economies and takes up a central role in our societies. Communications increasingly occur via a variety of platforms and new applications running over the internet. Data centres and infrastructure supporting these platforms and services are usually spread across the globe and are operated by multinational private sector players with operations in various jurisdictions.

Technological developments make it easier to collect, sift, copy, store and process information on a large scale. Contributing to the potency of these developments is the capability to analyse the information and to access it for later use. The compilation and correlation of massive data stores allows for the creation of complete profiles on individuals, accountings of their movements and behaviours, and the determination of social circles. The overall scope and saturation levels of data generated by IT systems render it invaluable for not only the private sector players, but also governments in pursuing law enforcement and national security interests.

Governments[1] are keen on gaining access to IT systems and to the communications conducted through, and the data retained in, those systems.[2] The nature of the information is varied, including for example, GPS data, health data, phone calls, email accounts, and information on usage of internet and social media.

In order to examine this data, governments may seek (1) direct access to private sector databases or networks; or (2) access mediated by the companies that maintain the databases or networks.

Often multiple stakeholders are involved, reflecting several interests and a variety of rights, including rights of privacy and property rights. Government attempts to obtain access or receive information, as well as the responses of the private sector to such attempts, raise complex legal issues, depending on the specific socio-political context and the domestic legal traditions. Where the access process spreads across various jurisdictions, a broad variety of national laws and spheres governed by international public law are implicated.

The right to respect for a person's privacy is the overarching international human right that is at issue with regard to government access to personal data. Unsurprisingly, many governments are under a duty to uphold this right, thus raising the need to balance the right to privacy with governmental interests and obligations under other provisions in domestic and international law.[3]

The technology and means used to facilitate the collection of data and surveillance of people has multiplied to the point that society and lawmakers have been unable to keep up.[4] Lack of clarity on laws

1 As used in this paper, the term 'government' has a broad meaning and refers to any state agency, administrative body, police authority, and in general, any entity provided with public powers.

2 Access is used to refer broadly to all access by relevant authorities, recognising that the rules may be different depending on who is accessing the information.

3 International legal instruments providing for a 'right to privacy' include: the United Nations, International Covenant on Civil and Political Rights, Art 17; Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) Art 8; and Charter of Fundamental Rights of the European Union [2012] OJ C 326/12 Art 7. Domestic instruments can similarly provide for a right to privacy. For example, Privacy Act 1988 (Australia), which provides a framework for protecting individuals' information privacy; Human Rights Act 1998 (UK), which gives domestic effect to the right to privacy guaranteed by the ECHR; and the Brazilian Federal Constitution of October 1988, which protects the right to privacy, including the secrecy of telephone and data communications.

4 M Rigoglioso, 'Civil Liberties and Law in the Era of Surveillance', [2014] Issue 91 *Stanford Lawyer* https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance accessed 12 August 2018.

regulating and balancing government interests and the other rights in play has attracted public attention and spread insecurity among society, business entities and governments. However, there has been little progress in terms of a unified global response to government access to IT systems.

The International Bar Association's (IBA) Legal Practice Division set up the Task Force on Government Access to IT Systems in October 2017, consisting of members from the committees of the IBA Intellectual Property, Communications and Technology Law Section to analyse these issues and draw up a set of working principles aimed to set a framework to reconcile the different rights and interests involved. This report provides the Task Force's assessment based on the considerations of this topic in different jurisdictions (Australia, Brazil, China, European Union, Russian, United Kingdom and the United States) and offers a set of working principles, detailed in Appendix A, for balancing government access to IT systems and fundamental rights.

Chapter 1: Accessing IT systems

Governments seek to preserve and use information resources through a variety of means, including data retention requirements,[5] data preservation orders[6] and the facilitation of access to stores of information.[7] Commonly, this is achieved through the application of legislative policies to electronic communications providers who generate the relevant data.

This legislation may directly require electronic communications service providers to collect, retain and provide access to relevant data for government aims. For example, the Investigatory Powers Act 2016 in the UK provides for access to content and communications data by public authorities after the data is collected by service providers. Provisions for access also exist in instruments that govern the use of data more generally. For example, the European Union Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) provides that its Member States should prohibit listening, tapping, storage or other kinds of interception or surveillance of communication and related traffic data, unless (1) the users have given their consent; or (2) there is a legal authorisation in accordance with Article 15.[8] The latter provision allows Member States to adopt legislative measures restricting the users' rights when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (ie, state security), defence, public security, to promote the prevention, investigation, detection and prosecution of criminal offences or prevent the unauthorised use of the electronic communication system.[9]

In order to gain access to relevant data held by service providers, governments utilise a variety of mechanisms. Those mechanisms can be facilitated through voluntary or compulsory cooperation with

---

5 In the European Union, Directive 2006/24/EC of the European Parliament and of the Council on the Retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC 2005 (2006) OJ L105 provided for the retention of data for periods of up to 24 months. This directive was invalidated following the Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER. Subsequent to this, individual States have updated and amended their data retention policies. See Investigatory Powers Act 2016 (UK); and Loi du 29 mai 2016 relative aux communications électroniques (Belgium). Jurisdictions outside the EU also provide for data retention in domestic instruments. See: Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 of Australia.

6 Data preservation (sometimes referred to as a quick freeze) is applied once a preservation order is issued and is utilised to prevent loss or modification to data. In contrast to data retention, which is applied to data processed by a service provider regardless of a link to a specific event or crime, data preservation occurs after an event has occurred. See Convention on Cybercrime (23 Nov 2001) Europ TS No 185 art 16-17, www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 accessed 12 August 2018.

7 At EU level, retention and access were treated separately with retention found in the invalidated Directive 2006/24/EC (Data Retention Directive) and specific access provisions left to individual Member States. The individual State positions regarding access will be discussed throughout this paper.

8 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data in the electronic communications sector (E-Privacy Directive) (2002) OJ L201. Recognising that the E-Privacy Directive as it stands has not kept pace with the evolution of technological and market realities, thereby resulting in inefficient protection of privacy in relation to electronic communications, a new e-Privacy Regulation is being drafted at EU level. See: Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (2017) 2017/0003(COD). It is expected that the new e-Privacy Regulation will come in to force in 2020.

9 These provisions are similarly replicated, and indeed expanded upon, in Regulation 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 (General Data Protection Regulation) Art 23 and Directive 2016/680/EC 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (2016) OJ L119 Art 15.

electronic communications service providers.[10] Governments may also obtain access without the cooperation of these providers through 'equipment interference', in common parlance, hacking.[11] By facilitating access, these tools enable both mass and targeted surveillance measures.

Mass surveillance is an indiscriminate and broad power, often justified using 'needle in a haystack' rhetoric. Large amounts of data are collected and retained, and governments seek subsequent access to these large data stores. The data may be derived from positive obligations to retain certain categories of data, from direct equipment interference, or from upstream surveillance programmes. The type of data that is subject to mass surveillance may be classed as either content data or 'metadata'. Content data has been defined as 'anything that might reasonably be considered to be the meaning of a communication'.[12] Metadata is data that serves to provide context or any form of additional information about other types of data.[13] It is the who, where, when and how of a communication but omits the content of what is said. Metadata is broadly classed into three areas: traffic data, location data and subscriber information.

Traffic data is that data which can be used to identify the person, device, location or address from which a communication is transmitted.[14] It is also used to identify the technical system which enables the transmission of the communications.[15] Location data is data that concerns the movement of individuals elicited from mobile and connected devices. This enables the compilation of a cache of personal information that individuals carry with them on a day-to-day basis. The traditional mechanisms for gathering such data would have been through targeted active surveillance by law enforcement or through the use of devices such as GPS trackers attached to vehicles. These powers were limited by practical concerns; it was not possible to follow a person everywhere. Location data has altered this, creating a new source of data, particularly through the functions of smartphones that accompany the individual most of the time. Location data is further enhanced by individuals' use of over the top (OTT) services such as social media platforms and search engines that can reveal the user's location.[16] Service use and subscriber information represent the third category of communications data. Service use information relates to the frequency and time a person used a service and which service they used. Subscriber information relates to all the other information that the customer provides, such as their address, telephone number, email address, etc, which is necessary in order for them to receive the service.

The most common form of metadata currently accessed relates to phone calls – the type of data gathered provides information such as the time, duration and the numbers of both the caller and the recipient of the call. In 2017, it was estimated that the US National Security Agency (NSA) collected over 534

---

10 For example, in the United Kingdom, until the Data Retention (EC Directive) Regulations 2007 (and now governed under the Investigatory Powers Act 2016), data retention for subsequent law enforcement access was governed by voluntary agreements with service providers under the Anti-Terrorism Crime and Security Act 2000. In the United States, voluntary arrangements existed between companies such as AT&T and Yahoo and the NSA. These were subsequently disclosed to the public in the Snowden revelations of 2013, See Angwin et al, 'AT&T Helped US Spy on Internet on a Vast Scale' *New York Times* (15 Aug 2015) www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html accessed 14 August 2018.

11 In the EU, six Member States possess specific legal frameworks related to the use of hacking techniques by law enforcement. Among these are the United Kingdom, which provides for 'equipment interference' in the Investigatory Powers Act 2016. Other relevant jurisdictions such as Australia and the US do not explicitly provide for hacking in legislation, but inferences have been made that permit law enforcement to utilise these mechanisms. See Telecommunications (Interception and Access) Act 1979 (Australia).

12 Investigatory Powers Act 2016 s 261(6).

13 Bruce Schneier, *Data and Goliath* (WW Norton & Co, 2015) 23.

14 See European Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) (2002) OJ L201 Art 2(b).

15 *Ibid.*

16 David Anderson Q.C., *A Question of Trust* (Stationary Office, 2015) p 56.

million records about American phone calls.[17] The high rate of collection regarding this material is closely linked to its investigative value. In the UK, for example, this type of data has played a role in every counterterrorism operation over the past decade and has been used as evidence in 95 per cent of all serious organised crime cases.[18] The prevalence of metadata in criminal investigations and national security cases can be explained in part by the lower thresholds that govern access to this type of data. In the UK, metadata may be accessed upon approval from a designated person within a law enforcement agency; there is no warrant requirement or judicial authorisation needed for access.[19] Similarly, in Russia there is no requirement for a warrant to be obtained to gain access to communications data.[20] The relatively low thresholds for access, coupled with the expansive nature of communications data make it a valuable tool for governments.

It is argued that mass surveillance enabled by the collection of metadata represents the biggest invasion of privacy and thus the most significant intrusion on human rights. Courts have held that retention and access of this data can represent an unjustified interference with privacy.[21] The vast majority of the people whose communications data is collected, are likely to be ordinary citizens with no connection to any wrongdoing. Some have even argued that these powers are counterproductive, and that the massive amounts of data generated makes it more difficult to spot terrorist activities and those guilty of crimes.[22]

In contrast to the bulk collection and retention of metadata, targeted surveillance represents the specific collection of data from people, groups of people or entities that have been identified as targets of investigation. It is a key tool for achieving the aims of law enforcement and national security agencies. Targeted surveillance aims to penetrate the networked devices and/or infrastructures of specific people, groups of people or entities through targeting phones, computers, and personal accounts including social media and cloud sharing accounts.[23] In most states, targeted surveillance can only legitimately proceed once applied for through the established processes.[24] This will typically require the approval of the authorisation from an independent or judicial body; absent this approval process, government access is likely to represent a violation of privacy rights. Extant case law in both the US and EU emphasises the

17 Niall McCarthy, 'NSA Triples Collection of U.S. Phone Records' (2018) *Forbes* www.forbes.com/sites/niallmccarthy/2018/05/07/nsa-triples-collection-of-u-s-phone-records-infographic/#6c23d3a03862 accessed 14 August 2018

18 Regulation of Investigatory Powers Act Consultation: Acquisition and Disclosure of Communications Data and Retention of Communications Data Codes of Practice (Home Office, 2014).

19 This has been amended as a result of The Investigatory Powers (Codes of Practice and Miscellaneous Amendments) Order 2018, SI 2018/905 and the draft Data Retention and Acquisition Regulations 2018. These instruments require that communications data must be accessed for the purposes of fighting serious crime. Furthermore, an independent authorising body, the Office for Communications Data Authorisations (OCDA) has been created to approve applications for access to this type of information. As of the time of writing, the Office has yet to come in to effect.

20 Yarovaya Law 2016 (Закон Яровой) (Rus) 374-FZ and 375-FZ.

21 See the cases of Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER; Joined Cases C-203/15 Tele2 v Post-och telestyrelsen & C-698/15 *Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970; *Malone v United Kingdom* (1984) 7 EHRR 14; *Kennedy v United Kingdom* App no 26839/05 (ECtHR, 18 May 2010); and *Liberty and Others v the United Kingdom*, 1 July 2008, no 58243/00; *Big Brother Watch & Ors v United Kingdom* App no 58170/13 (ECHR 13 Sept 2018).

22 Silkie Carlo, 'The case for targeted surveillance', Liberty (UK, 28 January 2016) www.liberty-human-rights.org.uk/news/blog/case-targeted-surveillance accessed 20 August 2018.

23 Ron Deibert, 'Journalism After Snowden: The Growing Digital Threat' (Global Investigative Journalism Network, 13 June 2017). https://gijn.org/2017/06/13/journalism-after-snowden-the-growing-digital-threat-to-the-press accessed 20 August 2018.

24 For instance, Australia has State, Territory and Commonwealth laws that regulate the use of surveillance devices. However, the laws also provide for the application for, and issue of, warrants to conduct surveillance by law enforcement officers; monitoring and oversight mechanisms; public interest exceptions; conditions for the admissibility of information obtained under surveillance as evidence; and restrictions on the manufacture and supply of surveillance devices. For example, under the Surveillance Devices Act 2004 (Cth) (SDA), law enforcement agencies, including the Australian Crime Commission and the AFP, can apply for a surveillance device warrant, which authorises the installation of a surveillance device on a premise, specified object or person. Furthermore, Art 5 of the European e-Privacy Directive provides that member States should prohibit listening, tapping, storage or other kinds of interception or surveillance of communication and related traffic data, unless the users have given their consent or unless legally authorised to do so in accordance with Art 15(1).

need for such authorisation.[25] In determining whether to permit access, the authorising body must assess whether the access satisfies the requirements of necessity and proportionality.[26]

Some argue that a distinction between mass and targeted surveillance is superficial.[27] Distinguishing between targeted and mass surveillance relies on a formal separation between corporate and government surveillance – or public and private surveillance. The nature of the technology being used means that intermediaries frequently serve as the logical gatekeepers for the information. As a result, private actors are increasingly being called upon to augment the surveillance capabilities of governments.[28] While public and private entities may extract different value from the data gathered in the surveillance, the invasion of privacy remains.[29] The increasing use of governmental access, whether targeted or broad in scope, creates a feedback loop; as governments become more dependent on the data generated, they develop a stake in facilitating more data collection.[30]

25 *Riley v California* 134 SC 2473 (2014); *Carpenter v United States* 585 US (2018); Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER; Joined Cases C-203/15 *Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970.

26 United Nations Special Rapporteur (2014) Report of the special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. General Assembly A/69/397 https://undocs.org/A/69/397 accessed 21 July 2020. .

27 Seda Gürses, Arun Kundnani & Joris Van Hoboken, 'Crypto and empire: the contradictions of counter-surveillance advocacy', 2016 38(4) *Media, Culture & Society* 576–590 http://journals.sagepub.com/doi/abs/10.1177/0163443716643006 accessed 12 August 2018.

28 Kevin Haggerty and Richard Ericson, 'The Surveillant Assemblage' (2000) 51(4) *Brit J of Sociology* 606.

29 *Ibid.*

30 Niva Elkin-Koren and Eldar Haber, 'Governance by Proxy: Cyber Challenges to Civil Liberties' (2201) 82 *Brooklyn L R* 105, 144.

Chapter 2: Provisions for retaining data

To fully understand the scale and scope of government access to IT systems, it is first necessary to examine the provisions that enable the creation of large pools of data that can then be accessed. Since the terrorist attacks of 11 September 2001, there has been an increased focus on terrorism and national security in domestic policy, leading to legislative developments which permit extended retention of data. In this context, data retention is the collection and storage, for a set period of time, of information generated through telephone and online communications. This time period is longer than the period for which the data would be kept purely for business purposes, such as billing and engineering.[31] Retention in this regard takes the form of an obligation on electronic communications service providers and providers of OTT communication services to retain data longer than they would for business purposes, in order to facilitate access by approved agencies. These provisions may relate to those providers of the basic network infrastructure, such as broadband and traditional telecommunications companies. Furthermore, legislative developments have expanded the application of these retention requirements to providers of OTT communications services,[32] which operate on top of the traditional network infrastructure (eg, WhatsApp, Skype). Data retained may never be accessed; it is merely the possibility that it may be that means retention is required. Further, it encompasses all service users. It is a blanket measure that occurs irrespective of individual suspicion or judicial authorisation. This aspect can be contrasted with the concept of data preservation, which typically occurs following the issuance of a warrant or a subpoena requiring a service provider to keep particular data about a specified individual for a set period of time.

Data retention meets the aims of government by enabling the construction of trails of evidence leading up to an offence and to corroborate other forms of evidence on the activities of suspects.[33] Discourses around retention frame it as a mechanism to increase security without significant downsides; proponents use language to moderate the debate around data retention framing it in non-controversial terms that liken it to nothing more intrusive than a phone bill.[34] Domestic policies reflect the desire to retain data. In Australia, a metadata retention law came into effect in April 2017. The provisions under this law require telecommunications companies to store customer metadata for at least two years.[35] The Australian Act is similar to the Investigatory Powers Act 2016 of the UK, which provides for comprehensive powers of data retention.[36] Expansive provisions regarding data retention are also evident in Russian law, which requires providers to store content for six months and metadata for three years.[37]

At EU level, the Madrid train bombings in 2004 and the 7/7 attacks in London in 2005 prompted the expansion of powers of data retention with the institutions noting that establishing rules on the retention of communications data was a priority, particularly due to its beneficial uses in the

31 European Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) (2002) OJ L201 Recital 26.

32 Investigatory Powers Act 2016.

33 European Commission, Evaluation report on the Data Retention Directive (Directive 2006/24/EC) (18.4.2011, COM (2011) 225 final, 2011).

34 Edgar A Whitley and Ian Hosein, 'Policy discourse and data retention: The technology politics of surveillance in the United Kingdom' (2005) 29 *Telecommunications Policy* 857, 860.

35 Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 Australia.

36 Investigatory Powers Act 2016 Part III.

37 See n 20 above.

investigation and prevention of terrorism and serious crime. 'Under these international dynamics, data retention went from something that was considered impractical and legally hazardous, to a regime that must be established to combat terror and organised crime'.[38] This took the form of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive). The Directive required the retention of certain types of data by communications service providers for up to two years. Directive 2006/24/EC was subsequently declared invalid in the joined cases of Digital Rights Ireland and Michael Seitlinger but data retention policies remain in many EU jurisdictions.[39]

Data retention provides the repository of information on which subsequent access is based. Historically, investigators would acquire required information, normally that of the call log of a telephone user, through an application to the electronic communications service provider. The information sought was that retained by the company for billing purposes. Changes in technology created issues with this process. As David Anderson QC noted in his review of investigatory powers in the UK, '[p]roliferating methods of communication, the fragmentation of providers, difficulties in attributing communications, changing business models, and increasing use of overseas service providers have all tended to make data more difficult to access'.[40] Domestic policies attempt to mitigate the difficulties occasioned by changing modes in technology in order to ensure that governments may access relevant data.

There are differences in the requirements and limitations that each state places on access to this retained data. For example, in Australia access occurs where it is authorised under law and it is reasonably believed that the disclosure of the information resulting from such access is necessary for the activities of an enforcement body.[41] In Russia, the Yaravoya amendments set forth data retention requirements for both the content and metadata of communications, mandating that the latter is retained for up to three years. The information must be stored inside Russian territory. Public authorities can then request access to this information as well as 'all other information necessary' without a court order.[42] In the UK, access to communications data can be provided on receipt of an application authorised by a designated person within the law enforcement body.[43] Such policies represent low bars for access to the IT system.

In contrast to the permissive access regimes of Russia and the UK, other jurisdictions demand additional requirements beyond internal authorisations on authorities before they can access the relevant information, thereby offering stronger safeguards for privacy. In Japan, the Act on Wiretapping for Criminal Investigations 1999 permits interceptions but only on receipt of a writ of execution by the court. Such an application is limited to serious crimes such as murder and organised crime. In the US, the Stored Communications Act section 2703 requires disclosure of the content of communications by the communications provider on condition that the governmental body obtains a warrant. In Brazil, a

38 See n 34 above, 857, 865.

39 In Belgium, data retention is still permitted but strict safeguards and security measures for the data have been added (Loi du 29 mai 2016 relative aux communications électroniques (Belgium)). Slovakia abolished the preventative blanket retention and storage of data and also introduced further safeguards for data (Act of the National Council of the Slovak Republic No. 351/2011 Coll. on the Electronic Communication (Zákon Národnej rady Slovenskej republiky č. 351/2011 Z.z. o elektronických komunikáciách), 14 September 2011).

40 David Anderson, 'A Question of Trust' (Independent Reviewer of Terrorism Legislation, June 2015) para 7.53.

41 Telecommunications (Interception and Access) Act 1979.

42 See n 20 above.

43 Investigatory Powers Act 2016 (UK) s 61(1).

judicial order is required for the government to access records.[44] In deciding whether to approve such an order, the judge must be provided with evidence as to the occurrence of an illicit act, an indication that the records will be useful for the investigation or probative instruction, and the request for records must relate to a specific period of time. The existence of such oversight prior to government access is an indication of the intrusive nature of the access and the need to balance that access with other rights and interests involved.

44 Marco Civil da Internet (2014) Law 12965/14 (Brazil) Art 22.

Chapter 3: Access to encrypted data

Maintaining data security and integrity is a fundamental data protection principle.[45] A key method by which companies maintain data security and integrity is through encryption technologies. Encryption converts messages, information, or data into a format that is not readable by anyone but the intended recipient.[46] In so doing, it protects the data against third party access or manipulation. Encryption technologies can be applied to data in transit, such as emails and messages, and to data at rest, including that which is stored on hard drives or cloud services. When properly implemented, encryption enhances the security of digital services such as those that are used for communicating, online shopping, banking and protecting critical public infrastructure.[47] In the digital world, encryption technologies are the norm.

Encryption technologies have implications for government access to data. Government officials frame encryption as a mechanism that frustrates the aims of law enforcement and security and intelligence agencies. Anonymous or encrypted communications make it difficult to investigate crimes, including those related to illicit drugs, child pornography, and terrorism. Governments advocate for installing capabilities into technologies that would permit backdoor access to systems or provide for decryption keys.[48] Calls for enhanced capabilities for governments to access encrypted data are often the result of terrorist attacks and other perceived threats to national security.[49] Such is the case with India's current policy on encryption, which is best understood as a response to the 2008 Mumbai bombings that left more than 170 dead and hundreds more injured.[50] As per the Indian Information Technology Act of 2008, the Indian Government can intercept, monitor or decrypt any electronic data for national security purposes.[51]

In addition to government acts to decrypt information, service providers may be called upon to decrypt the encrypted data themselves, and failure to do is punishable by imprisonment and/or a fine.[52] China similarly places an obligation on technology firms to help decrypt information.[53] Australian law mandates that, upon receipt of a warrant, technology companies must quickly provide decrypted communications to the relevant authorities.[54] A comparable trend can be seen in the US, with calls for IT companies to

45 Regulation 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 L 119/1 Art 5(1)(f) Personal data must be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

46 SANS Institute, 'History of encryption' (2001) www.sans.org/reading-room/whitepapers/vpns/history-encryption-730 accessed 18 August 2019.

47 Peter Swire and Kenesa Ahmad, 'Encryption and Globalisation' (2012) 13 Colum Sci & Tech L R 416, 453.

48 See the speech given by Prime Minister David Cameron on 12 January 2015 at the Conservative Party conference for the 2015 General Election and the speech given by James Comey, Director of the Federal Bureau of Investigation, on 16 October 2014, entitled 'Going dark: are technology, privacy and public safety on a collision course?', at the Brookings Institution, Washington, DC. At its 29 August 2018 Ministerial meeting in Australia, the 'Five Eyes' Intelligence Alliance (UK, US, Australia, New Zealand and Canada) issued a 'Statement of principles on access to evidence under encryption', under which: 'The Governments of the Five Eyes encourage information and communications technology service providers to voluntarily establish lawful access solutions to their products and services that they create or operate in our countries.' The statement went on to conclude that 'Should governments continue to encounter impediments to lawful access to information necessary to aid the protection of the citizens of our countries, we may pursue technological, enforcement, legislative, or other measures to achieve lawful access solutions'. [Australian Government of Home Affairs], 'Statement of Principles on Access to Evidence and Encryption' (29 August 2018) https://www.ag.gov.au/sites/default/files/2020-03/joint-statement-principles-access-evidence.pdf accessed 21 July 2020.

49 D Lee, 'Message encryption a problem – Rudd' (BBC News, 1 August 2017) www.bbc.com/news/technology-40788180 accessed 14 August 2019; The case of Apple v FBI is a significant example of encryption technologies being challenged in light of a terrorist attack.

50 See n 47 above, 416.

51 The Information Technology (Amendment) Act, No 10 of 2008, Acts of Parliament, 2009 (India) https://www.meity.gov.in/writereaddata/files/itact2000/it_amendment_act2008.pdf accessed 21 July 2020.

52 *Ibid*, s 69.

53 Counter-Terrorism Law of the People's Republic of China, passed by the 18th Session of the Standing Committee of the 12th National People's Congress on 27 December 2015.

54 Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Aus) Schedule 1.

develop effective ways to provide secure encryption for users while also providing secure legal access for law enforcement.[55]

In addition to direct obligations placed on companies to decrypt data, policies can dictate that companies incorporate technical capabilities to facilitate government access. In the US, this occurs through statutory obligations which require all telecommunications carriers to ensure that their equipment, facilities, or services which enable communications are able to intercept and deliver those communications to the government on receipt of a court order or other lawful authorisation.[56] Arguably this means that the telecommunications providers cannot encrypt communications in a way that would prevent them from satisfying this requirement.[57] In the UK, the Investigatory Powers (Technical Capability) Regulations 2018 require that service providers disclose data sought in an intelligible form, with any additional electronic protections applied to it removed.[58] Other jurisdictions impose technical limitations by mandating the disclosure of encryption keys to the relevant authorities,[59] or requiring that encryption keys do not exceed an easily breakable 40-bit key length.[60]

While the aforementioned policies impose obligations on providers to assist authorities and provide access, the encryption technology itself can render this impossible. Take the example of end-to-end encryption utilised by popular messaging services WhatsApp and Telegram. Utilising this technology, the encryption keys are generated by the users' own devices; the communications providers are not able to intercept or read the content sent via their platforms. The providers are therefore unable to decrypt the information to provide access to law enforcement. The use of the technology, and the subsequent limitation on the powers of access, have resulted in legal challenges being brought against these companies. For example, in the Telegram case, the Russian Federal Security Service ('FSB') demanded that Telegram disclose its universal encryption key on all user correspondence.[61] Telegram refused on the basis that the encryption keys are generated on the users' devices and it is therefore technically impossible for the provider to disclose the information. Ultimately, the Russian Court issued an order to ban the messaging app.[62] Similar legal challenges have occurred in Brazil, wherein the court system is being used to implement encryption technology. In recent legal challenges, the Brazilian government has called upon the messaging platform WhatsApp to decrypt communications sent over the app. The courts have responded by blocking the popular app until the encryption is removed.[63] However, these rulings have been found to be disproportionate due to the impact of banning millions of WhatsApp users in Brazil.

While extant legislative policies indicate a desire to limit encryption to promote government access, any such limitation must be balanced against the resultant risks to cybersecurity and fundamental

---

55 William Barr, 'Keynote Address at the International Conference on Cyber Security' (New York, NY 23 July 2019) www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber accessed 14 August 2019.

56 Communications Assistance for Law Enforcement Act (CALEA) 1994 s 103(a) 47 USC ss 1001-1002.

57 However, under CALEA 1994 s 103(b)(3) service providers cannot be required to decrypt communications that are encrypted by the subscriber or the customer. It only applies to the technologies applied by the service providers themselves.

58 Investigatory Powers (Technical Capability) Regulations 2018 SI 2018/353 Schedule 2 Part 1(8).

59 See n 20 above: Under this law, social media providers, as well as messengers and email clients that are using data encryption are mandated to share their encryption key with the FSB.

60 The Government of India, Ministry of Communications and IT, Licence Agreement for Provision of Internet Services (2007): service providers may not deploy 'bulk encryption' on their networks, while the law has also restricted individuals from using encryption greater than an easily breakable 40-bit key length without prior permission and required anyone using stronger encryption to provide the government with a copy of the encryption keys.

61 Scan of the FSB request – https://vk.com/doc1_451499493?hash=f45613990541c82af8&dl=136a40c575bfa82136.

62 Neil MacFarquhar, 'Russian Court Bans Telegram App After 18-Minute Hearing' New York Times (New York, 13 April 2018) www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html accessed 24 August 2019.

63 Vinod Sreeharsha, 'WhatsApp Blocked in Brazil as Judge Seeks Data' New York Times (2 May 2016) www.nytimes.com/2016/05/03/technology/judge-seeking-data-shuts-down-whatsapp-in-brazil.html accessed 24 August 2019.

rights. Encryption is a pre-eminent element of cybersecurity. It not only protects the confidentiality of communications but ensures the integrity of financial systems and public infrastructure as well. As one privacy scholar explains, 'any legal regime that prohibits the use of strong encryption thus significantly undermines and harms its cybersecurity'.[64] It is not possible to build backdoors or lower encryption key requirements in a manner that will only benefit the government. Any vulnerability or lower security threshold incorporated into a system will be open to attack from malicious actors. As a cybersecurity expert succinctly states: 'you can't build a backdoor that only the good guys can walk through… You're either vulnerable to eavesdropping by any of them or you're secure from eavesdropping by all of them'.[65] Introducing vulnerabilities into systems to permit government access also has implications for private actors. If a company introduces technology that decreases its data security and results in a breach, the company could incur civil and criminal penalties, suffer damage to its brand, loss of consumer trust and a drop in market value.

Policies that mandate decryption may also infringe fundamental rights of privacy, freedom of expression, freedom of speech and freedom of association. Encryption and anonymity enable individuals to express their thoughts freely and without fear of sanction. The risk of online activity being disclosed can deter individuals from accessing information.[66] Interference with digital communications may enable states to identify dissidents and political opponents. Vital components of a democratic society, such as a free press, benefit from the existence of encryption measures which enable sources and whistleblowers to communicate anonymously.

Any interference with these rights must be limited. As the UN Special Rapporteur on freedom of expression concludes: 'a common threat in the law is that, because the rights to privacy and to freedom of expression are so foundational to human dignity and democratic governance, limitations must be narrowly drawn, established by law and applied strictly and only in exceptional circumstances. Restrictions on encryption and anonymity that enable individuals to exercise their rights must therefore only be interfered with if the interference is provided by law, necessary, and proportionate to the aim to be achieved'.[67] Europol has recognised the need for provisions on encryption to be limited and proportionate in line with these standards, noting that whilst the powers may be proportionate with respect to an individual suspect, there is a risk of collateral intrusion.[68] As a result, the focus should be on specific and limited access to encrypted information rather than the diminishment of the overall encryption technologies.

In balancing the demand for decryption technologies with interferences with fundamental rights, it is worth examining whether the aims of law enforcement and security and intelligence agencies could be met by less intrusive means. In this regard, it is worth noting that governments currently possess a wide range of alternative tools, such as wiretaps, location data, data-mining, and traditional physical surveillance which are used to great effect in the investigation and detection of crimes and national security threats. Access to data can be achieved through a variety of tools that do not require companies to

64 Peter Swire n(47) 458.

65 Bruce Schneier, 'US Enables Chinese Hacking of Google' CNN (23 January 2010) edition.cnn.com/2010/OPINION/01/23/schneier.google.hacking/index.html accessed 16 August 2018.

66 David Kaye, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UNHRC 29/32) 22 May 2015, 8.

67 *Ibid.*

68 Europol, 'On lawful criminal investigation that respects 21st Century data protection, Europol and ENISA Joint Statement (20 May 2016) www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection accessed 15 August2016.

remove encryption, including: access to metadata and unencrypted data;[69] policies that require individuals to provide their encryption key;[70] targeted interception tools; and other technological capabilities to intercept passwords, access documents or record keystrokes.[71] The loss of legitimate access to data caused by encryption can therefore be offset by new technologies that pose less risk of collateral intrusion.

Accepting that encryption is crucial to the security of services upon which individuals, businesses and governments rely, and acknowledging that it is not possible to create special access that will only be available to government authorities, it is proposed that where possible, states should utilise other technical tools they possess to obtain the necessary data, in accordance with the provisions laid down in law. Any policies that restrict encryption must be undertaken on a case-specific basis that meet the requirements of legality, necessity and proportionality and are subject to judicial approval. Such an approach must be applied consistently across jurisdictional boundaries, as the global nature of communications would render them only as secure as the least trusted country.

69 For example, in the case of WhatsApp, while the content of the messages may be encrypted, the metadata is not.

70 Information Technology Act 2000 as amended by the Information Technology (Amendment) Act 2008 (India) s 69 requires individuals to decrypt their data if called upon; Australia Crimes Act 1914 Section 3LA (inserted by the Cybercrimes Act 2001) requires that a person provide any information or assistance to allow a constable to access data in an intelligible form; United Kingdom RIPA 2000 Part II requires a person to produce the data in an intelligible format upon receipt of a judicial authorisation.

71 Notably this is what occurred in the case of *In the Matter of the Search of an Apple iPhone Seized during the Execution of a Search Warrant on a Black Lexus IS300,* California License Plate 35KGD203 (16 Feb 2016), commonly known as Apple v FBI, wherein the FBI ultimately accessed the encrypted data through other means without Apple having to install the backdoor access so demanded.

Chapter 4: Impact on rights of individuals

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) is the most important legally binding treaty provision guaranteeing the right to privacy at the universal level.[72] It provides that 'no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home and correspondence, nor to unlawful attacks on his or her honour and reputation'. It further provides that 'everyone has the right to the protection of the law against such interference or attacks'. Other international human rights instruments contain similar provisions. Among these are the European Convention on Human Rights (ECHR) which protects the right to private, family and home life and correspondence under Article 8 and the European Union Charter on Fundamental Rights, which guarantees the right to privacy and data protection under Articles 7 and 8 respectively. Furthermore, laws at the regional and national levels reflect the right to respect for their private and family life, home and correspondence. In these instruments, the confidentiality of correspondence and communication has been given special protection beyond the mere protection of personal data and privacy.[73]

For example, the Constitution of the Federative Republic of Brazil, which serves as the highest legal instrument in Brazil, recognises the rights to privacy and intimacy as fundamental rights.[74] Such constitutional protection provides a strong barrier to the enactment of abusive laws – which pertain to an inferior hierarchic level than the Constitution – that are meant to give governments carte blanche to access individuals' data. Similarly, in *Justice K S Puttuswamy (Retd) and Anr v Union of India*, the Supreme Court of India held that privacy, while not explicitly provided for in the Indian Constitution, is intrinsically attached to Article 19(1)(a) (freedom of speech and expression) and Article 21 (right to life and personal liberty). However, this is not the case in every jurisdiction. Other countries, such as Australia, do not have a federal bill of rights or provide broad constitutional protections such as freedom of expression and right to privacy.

The right to privacy is not an absolute right and limitations to the right to privacy may be pursued for legitimate purposes. In the case of access to data, the grounds most often relied upon by the state are national security and the fight against crime. Any limitation must be in accordance with law, proportionate and strictly necessary. Once an individual is under suspicion and subject to formal investigation by intelligence or law enforcement agencies, that individual's data may be accessed for entirely legitimate counterterrorism and law enforcement purposes. Article 17 of the ICCPR does not contain a specific limitation clause outlining the circumstances in which interference with the right to privacy may be permitted, although, it is universally understood that such measures can be taken provided that: they are authorised by domestic law that is accessible and precise and that conforms to the requirements of the Covenant; they pursue a legitimate aim, and meet the tests of necessity and proportionality.

---

72 United Nations, International Covenant on Civil and Political Rights, Art 17.

73 See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data in the electronic communications sector (E-Privacy Directive) (2002) OJ L201; Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (2017) 2017/0003(COD).

74 The Constitution of the Federative Republic of Brazil, as of 1988, sets out that the privacy, private life, reputation and image of the persons are inviolable, and it provides for the right to compensation for pecuniary and moral damages resulting from their violation (Art 5, X). Also, the Constitution states that the secrecy of correspondence and of telegraphic, data and telephone communications is inviolable (Art 5, XII). Fourth Amendment of the US Constitution provides protection from unreasonable searches and seizures without probable cause.
'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'

The prevention, suppression and investigation of acts of terrorism, for example, amount to a legitimate aim for the purposes of Article 17. Terrorism can destabilise communities, threaten social and economic development, fracture the territorial integrity of states, and undermine international peace and security. Under Article 6 of the ICCPR, states are under a positive obligation to protect citizens and others within their jurisdiction against acts of terrorism. One aspect of this obligation is the duty to establish effective mechanisms for identifying potential terrorist threats before they have materialised. States discharge this duty through the gathering and analysis of relevant information by intelligence and law enforcement agencies. Moreover, since terrorism is a global activity, the search for those involved must extend beyond national borders. The prevention and suppression of terrorism is thus a public interest imperative of the highest importance and may in principle form the basis of an arguable justification for intrusive access regimes.

Governments seeking to balance access to data with the protection of rights must walk a fine line between legitimate and unlawful/arbitrary interferences. To ensure a certain quality of Article 17 of the Covenant: (1) the measure must have some basis in domestic law; (2) the domestic law itself must be compatible with the rule of law and the requirements of the Covenant; and (3) the relevant provisions of domestic law must be accessible, clear and precise.

Technological developments and the data they produce pose a significant challenge to the legality requirements of both international and domestic instruments. Many states still rely on outdated domestic laws that were designed to deal with much more primitive forms of technology. Applying the same policies to technologies that are quantitatively and qualitatively different in the amount of detailed personal information they can provide often means the protections for privacy are considerably weaker. Recent case law has recognised the highly revealing nature of the data generated by these technologies and the need to distinguish it from previous types of information sought by public authorities. For example, in the case of *Riley v California* the US Supreme Court held that 'a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form'.[75]

Domestic laws governing the interception of communications should be updated to reflect modern forms of digital surveillance that are far broader in scope, and involve far deeper penetration into the private sphere, than those envisaged when much of the existing domestic legislation was enacted. The absence of clear and up-to-date legislation creates an environment in which arbitrary interferences with the right to privacy can occur without commensurate safeguards. Explicit and detailed laws are essential for ensuring legality and proportionality in this context. They are also an indispensable means of enabling individuals to foresee whether, and in what circumstances, their communications may be the subject of surveillance. A regular review of such laws is required to avoid their becoming outdated. International coordination should prevent too much fragmentation and distortion in the level of protection in a data economy that is becoming truly global.

While the right to privacy is the core right affected by government access to data, other rights can be affected as well. These include the rights to freedom of opinion and expression, wherein government access may result in individuals being unable to fully exercise these rights for fear of sanction. Linked to

75 *Riley v California* 134 SC 2473 (2014).

this are rights concerning freedom of peaceful assembly and association. Access to data has the potential to reveal links between individuals, thereby impacting on the exercise of this right. The UN Special Rapporteur on privacy similarly noted that additional rights, such as the right to health, may be impacted by the access provisions, 'for example, where an individual refrains from seeking or communicating sensitive health–related information for fear that his or her anonymity may be compromised'.[76] Any interference with these rights must be balanced against the objectives to be achieved.

76 UNGA, Resolution adopted by the General Assembly on 18 Dec 2013 on The right to privacy in the digital age, (2013) A/RES/68/167 para 14.

Chapter 5: Balancing rights of individuals and government interests

In recent years, legislation from across the globe has enabled governments to access data extensively and to use such data to build more detailed profiles on citizens, often free from any real scrutiny from judicial and oversight mechanisms. When developing these policies, due regard must be had for the way in which these powers will impact on fundamental rights and how to achieve an effective balance in this area. The intrusions with privacy occasioned by government access to IT systems may be offset by oversight mechanisms that ensure the actions prescribed by the state comport with the necessary rule of law values. As such, any measures that interfere with fundamental rights must be assessed against the principles of legality, necessity and proportionality.

With regard to legality, this principle requires that the measure have a basis in domestic law that is adequately accessible and foreseeable, thereby enabling the individual to identify, with sufficient precision, when their conduct may be subject to the access provisions. In the context of surveillance measures, precedent requires that '[t]he domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures'.[77] This does not require that individuals be provided with detailed information about the surveillance regimes utilised to capture their data for law enforcement purposes. In matters wherein providing individuals with information might frustrate the intended purpose of the act, that is, by giving suspects detailed information on when their data may be targeted, the act may limit the disclosure as necessary to ensure the aims of national security and the prevention and detection of crime.[78]

Mechanisms that permit interferences with fundamental rights by enabling the collection and processing of information must be governed by precise rules pertaining to the scope and application of the measures, as well as safeguards regarding access, usage, procedures and destruction.[79] However, the requirements for investigatory measures to be 'in accordance with law' in line with the relevant jurisprudence does not require the precise rules and safeguards to be explicitly set forth in statute; secondary or non-binding instruments may satisfy this requirement. At EU level, the courts have accepted that the Executive has discretion to provide for these elements in secondary instruments rather than the substantive law.[80] The ability of individuals to access information about the procedures that may be applied to them is crucial for the rule of law; individuals must know which laws they are bound by and when they may fall afoul of those laws.

---

77 See: *Malone v United Kingdom*, 2 Aug 1986 paras 66-68; *Rotaru v Romania* [GC], App no 28341/95 para 55 ECHR 2000-V; *Amann v Switzerland* App no 27798-95 ECtHR 2000-II; *Kruslin v France*, 24 April 1990, para 27, Series A no 176-A; *Lambert v France*, 24 August 1998, para 23, Reports 1998-V; *Perry v the United Kingdom*, no 63737/00, para 45, ECHR 2003-IX; *Dumitru Popescu v Romania* (no 2), no 71525/01, para 61, 26 April 2007; Association for European Integration para 71; *Liberty and Others v the United Kingdom*, 1 July 2008, no 58243/00 para 59; *Szabo & Vissy v Hungary* App no 37138/14 (ECtHR, 12 Jan 2016) para 59.

78 See *Szabo & Vissy v Hungary* App no 37138/14 (ECtHR, 12 Jan 2016) para 62: 'Foreseeability in the special context of secret measures of surveillance…, cannot mean than an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly'.

79 *Kruslin v France*, 24 April 1990 Series A no 176-A paras 33 and 35; *Rotaru v Romania* [GC], App no 28341/95 ECHR 2000-V para 55; *Weber & Saravia v Germany* App no (54394/00) ECHR 29 June 2006; *Liberty and Others v the United Kingdom*, 1 July 2008, no 58243/00 paras 62-63; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER para 99.

80 *Malone v United Kingdom* (1984) 7 EHRR 14 para 68.

In addition to meeting the standards of legality, provisions governing the collection and processing of data that result in interferences with fundamental rights must be necessary and proportionate. For example, the ruling in *S and Marper v United Kingdom* requires that where the interference is with individuals' personal data, and involves the use of potential cutting-edge technologies to invade privacy, the criteria of 'necessary in a democratic society' must be interpreted as strict necessity.[81] Strict necessity requires that the power must be necessary for 'safeguarding the democratic institutions, and moreover…, for the obtaining of vital intelligence'.[82] Similarly, any data collection policies, undertaken through secret means, which concern persons not suspected of involvement in a specific crime or posing a threat must be subject to a strict necessity test to justify an interference with the fundamental right.[83]

Concomitant with the requirement that the powers be strictly necessary is the condition that they be proportionate to the aim to be achieved. The requirement of proportionality is particularly important when considering the data tools as they indiscriminately relate to large swathes of the population in the absence of any reasonable suspicion that they have been involved in a crime. Due regard must be had for the principle of proportionality when derogating from and limiting fundamental rights.[84] In determining whether a provision goes beyond what is strictly necessary and proportionate, courts will assess what safeguards and oversight exist against abuse.

To protect the other rights and interests that are involved when governments are accessing data, there must be an element that objectively justifies such access. In other words, in order for individuals' personal data to be protected, indiscriminate access to such personal data should not be granted without a justiciable motive. General principles such as data minimisation – according to which personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed – should be taken into consideration while enacting laws that force certain service providers to keep a record of information for certain periods of time.[85]

The European Court of Human Rights (ECtHR) affirmed that the protection of personal data is of fundamental importance to a person's enjoyment of his/her right to respect for private and family life, as guaranteed under Article 8 of the ECHR. Therefore, national laws shall ensure that such data are:

- relevant – and not excessive – in relation to the purposes for which they are collected and/or stored;
- preserved in a form that allows identification of the data subjects for a certain limited period, no longer than the time required for the purpose for which such data are stored; and
- protected from misuse and abuse.[86]

81 *S and Marper v United Kingdom* App No 30562/04 and 30566/04 (ECHR 4 December 2008) para 73.

82 *Ibid.*

83 CoE, 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' CON (1985) 108.

84 C-73/07 Satakunnan Markkinapörssi and Satamedia [2008] EU:C: 727 para 56; C-92/09 and 93/09 Volker und Markus Schecke and Eifert [2010] EU:C:662 para 77; Case C-362/14 *Max Schrems v Data Protection Commissioner* (2015) OJ C351/14 para 92-96; Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER para 52.

85 Directive 2006/24/EC of the European Parliament and of the Council on the Retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC 2005 (2006) OJ L105.

86 *S and Marper v United Kingdom* App No 30562/04 and 30566/04 (ECHR 4 December 2008) para 103.

Such a principle was applied, for instance, in *L.H. v Latvia* (No 52019/07), where the applicant alleged that the collection of her personal medical data by a state agency – in this case, the Inspectorate of Quality Control for Medical Care and Fitness for Work ('MADEKKI') – without her consent had violated her right to respect for her private life. The ECtHR held that there was indeed a violation of Article 8 of the ECHR as the applicable domestic law had failed to indicate with sufficient clarity the scope of discretion conferred on competent authorities and the manner of its exercise. In particular, the ECtHR affirmed that Latvian law in no way limited the scope of private data that could be collected by MADEKKI, which collected medical data related to the applicant for seven years indiscriminately and without any prior assessment of whether such data could be potentially decisive, relevant or of importance for achieving the purpose for which such data has been collected.

In determining whether access satisfies the requirements of legality, necessity and proportionality, any limitations or safeguards placed on access must be assessed. Access provisions must ensure they protect the other rights and interests involved and reduce harm to a minimum. As highlighted above, national laws may provide that government holds the power to access or request private entities provide access to data only in case of necessity and in order to protect public interest. In general, governments may be required to obtain an authorisation from an independent third party – such as the judiciary – before being granted access to the data demanded. However, in case of exceptional urgency and as *extrema ratio*, governments may access IT systems and databases without prior authorisation.[87] Where access has been granted prior to any authorisation due to exigent circumstances, an ex post approval of such access by the independent third party is desirable.[88]

To guarantee that access is done in accordance with law, any access provisions should provide clear thresholds that must be met before the data can be accessed. One such threshold is constraining access to only those cases where such access is for the aim of investigating serious crime or issues of national security. This requirement is clearly established in the cases of the Court of Justice of the European Union (CJEU) in *Digital Rights Ireland* and *Tele2 and Watson* wherein, in addition to the requirement that retention or access cannot be organised in a general, non-discriminate way, it was clearly held that: 'Given the seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure'.[89] It is important to note the link between the seriousness of the interference and the objective of fighting serious crime. The CJEU has ruled that where the interference occasioned by government access is not 'serious', then the objective of preventing, detecting and prosecuting 'criminal offences' generally will be sufficient to justify the interference with fundamental rights which results.[90]

'Serious crime' is a subjective term and therefore requires defining. There is no single definition of 'serious crime'. Some States define it with regard to a minimum prison sentence, to the possibility of a

87 Stored Communications Act (US) 18 USC ss2702 which permits the voluntary disclosure of customer records to the government if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.

88 Investigatory Powers Act 2016 (UK) Part III.

89 See Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors* [2014] 2 All ER para 60; Joined Cases C-203/15 *Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970 para 102.

90 C-207/16 Ministerio Fiscal (2018) ECLI 788.

custodial sentence being imposed, or with regard to a list of specific criminal offences.[91] Still other states refer to 'serious crime' without defining it.[92] In order to ensure that the data accessed does only relate to 'serious crime', the CJEU has stated that the national legislation must be based on objective criteria that clearly define the circumstances and conditions when authorities will be authorised to access the data. 'In that regard, access can, as a general rule, be granted in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a 'serious crime', or of being implicated in one way or another in such a crime'.[93] As a result, any national legislation that does not limit access to objectives pursued in investigating and detecting 'serious crime' are open to legal challenge. This provision serves to limit the amount of data that can be accessed and ensures such access is only provided where necessary.

An interrelated issue in defining 'serious crime' is the blurring of distinctions between activities that would fall under this threshold, and those that fall under the remit of 'national security'. The state is afforded a wider margin of appreciation in cases of national security and the courts have recognised this. Where 'national security' is at stake, data access provisions may be broadened to people other than the specific targets.[94] However, permitting this additional access must be based on objective evidence that the data will contribute to the fight against a specific 'national security' threat. In countering these national security threats, enhanced cooperation between law enforcement and security and intelligence agencies is required; yet there must be strict organisational separation between law enforcement and intelligence agencies.[95] If the powers are to be exercised under the national security exemptions, the state should first prove that the threat cannot be met by processes of ordinary criminal law. Cases that blur the distinction between national security and serious crime need to critically assess whether the acts or threats under investigation truly fall under the national security ambit.

In addition to the purpose limitations that bound access to data to instances of serious crime or national security, requests for data should be circumscribed and limited in their scope. It is essential that the scope of access be clearly and specifically defined. Data should be retained and accessed only for the timeframe strictly necessary to achieve the aim pursued. There should be specific provisions set forth in statutes as to what the data can be collected and used for and how it is to be deleted after the necessary period of time. In addition, data minimisation processes can be used to limit the data collected and accessed. These minimisation rules can provide important protections for fundamental rights.

Data minimisation emphasises collecting less data ab initio. This can be achieved through the infrastructure, in the form of software and hardware that creates and utilises the data, and also by reliance on legal principles.[96] Further strategies to permit data minimisation should include technical access requirements that require multiple persons to oversee and authorise disclosure of the relevant

---

91 Commission, 'Evaluation report on the Data Retention Directive (Directive 2006/24/EC) COM (2011) 225 final 6. Ten Member States define serious crime in this manner: Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, the Netherlands, and Finland. For example, in Ireland, serious crime is defined in relation to offences punishable by imprisonment for a term of five years or more. [Communications (Retention of Data Act) 2011 Art 6.]

92 This is the case for Malta, Portugal and the United Kingdom which merely state: for the investigation, detection, and prosecution of serious crime. *Ibid.*

93 Joined Cases C-203/15 *Tele2 v Post-och telestyrelsen & C-698/15 Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970 para 118.

94 Fundamental Rights Agency, 'Surveillance by Intelligence services: fundamental rights, safeguards, and remedies' (2017) Vol 2, 22.

95 This is the case in the UK; other EU Member States fail to provide for strict organisational separation of intelligence and law enforcement, including Austria, Denmark, Finland and Ireland, where the body responsible for intelligence activities is officially part of the police and/or law enforcement authorities. [Ibid 28]

96 Lillian Edwards, 'Privacy and Data Protection Online: The Laws Don't Work?' in Edwards and Wealde (eds) *Law and the Internet* (Hart 2009) 468.

information from the company in possession of the data. This will ensure the information provided is limited to what is necessary.

To further limit interferences with fundamental rights regarding access, there should be provisions limiting the onward sharing of data once it is disclosed through a legitimate access request. The potential spread of data to authorities beyond those who obtained authorisation to access greatly increases the risk of collateral intrusions, data misuse and violations of privacy. The relevant individuals able to view and utilise the data must be confined to mitigate this risk. In practice, many domestic frameworks do not possess use limitations that limit the subsequent use of data collected for one legitimate aim from being used for another purpose. The UN Special Rapporteur on privacy notes that:

> 'the absence of effective use limitations has been exacerbated since 11 September 2001, with the line between criminal justice and protection of national security blurring significantly. The resulting sharing of data between law enforcement agencies, intelligence bodies, and other state organs risks violating Article 17 of the Covenant, because measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another'.[97]

Such 'use limitations' are accepted good practice to ensure the data accessed is only utilised for the approved purpose.

97 See n 76 above, para 27.

Chapter 6: Reach beyond territorial jurisdiction

At present, territorial jurisdiction and state sovereignty are important boundaries to governments' access to data. Data is often stored on servers abroad, ie, out of reach of domestic investigators. In response to this, some states have included in their domestic laws, provisions to allow for extraterritorial access to data. This is the case with the UK Investigatory Powers Act, wherein, targeted interceptions and authorisations to access communications data may be enforced outside the traditional jurisdiction of the UK.[98] These provisions can require a non-UK based telecommunications operator to give effect to a UK warrant or notice. In the US, under the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), a service provider who is subject to US jurisdiction may be required to produce data that the provider controls, regardless of where the data is stored at any point in time.[99]

Provisions that grant states the ability to access information held outside their traditional jurisdictions run counter to accepted principles of international law.[100]

In some cases, courts have applied creative theories to expand the territorial jurisdiction of investigators to order data from foreign entities, such as by relying on the fact that the information sought would then subsequently be used for an investigation taking place within the jurisdiction. Such theories are dubious and may in fact lead to a national court assessing worldwide jurisdiction.[101] Judges are presumed to lack the authority to unilaterally authorise extraterritorial searches and seizures.[102] In limited instances, courts have held that domestic jurisdiction may be extended to acts that were intended to have effect, and indeed did have such effect, on the territory of the state.[103] Such practices, while limited in their scope, are generally viewed as contrary to international comity and fairness, and may encourage confrontation between states, rather than cooperation. Yet, absent any legal agreement that permits extraterritorial access, measures to obtain data, taken within the territory of another state without their consent, would be considered illegal. However, the nature of data creates difficulties with traditional jurisdictional boundaries. Data typically does not reside in a single fixed, observable location. It moves frequently and easily for a variety of reasons, such as technical processing or maintenance. Furthermore, data is frequently copied and stored in more than one location to protect against malfunctions and to ensure the information is backed up.[104] Those seeking access may not be aware that the data is not within their jurisdiction or may seek access erroneously believing they have jurisdiction.[105]

In order to ensure they retained access to data, several states have incorporated data localisation measures into their domestic law. Such measures may include: rules preventing information being sent outside

98 Investigatory Powers Act 2016 ss41(1) and s(66).

99 Clarifying Lawful Overseas Use of Data Act 2018 (US) HR 4943.

100 Restatement (Third) of Foreign Relations Law in the United States § 432(2) (Am Law Inst 1987) ('A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state.'); James Crawford, *Brownlie's Principles of Public International Law* 478-79 (8th ed, 2012).

101 *Belgian Court of Cassation 1 December 2015, AR P 13.2082 N, RABG 2016, no 7, 485; Correctional Court of Mechelen* 27 October 2016, ME20.F1.105151-12.

102 Jennifer Daskal, 'The Un-territoriality of Data' (2015) 125 Yale L J 326, 354.

103 This is known as the 'effects doctrine' and is employed in the field of private competition law. As such, it is of limited direct influence on the practices of governments accessing IT systems that raise public law issues; but as a principle it may be instructive to see how it has been used to extend jurisdictional reach. See: *United States v Aluminium Co of America* (1945) 148 F 2d 416; *Re Wood Pulp Cartel* [1988] ECR 5193.

104 See n 102 above, 326, 368.

105 See the case of *United States v Gorshov* 2001 WL 1024026 (WD Wash 23 May 2001). Therein an FBI agent copied data from a computer in Russia. It was held to be an extraterritorial search. Russia similarly deemed it an extraterritorial search and filed criminal charges for hacking against one of the FBI agents involved.

the jurisdiction; rules requiring prior consent before the data is transmitted across borders; and rules requiring copies of information be stored domestically.[106] Often, the data localisation measures will relate to specific categories of data. For example, Australia prohibits the transfer of health records outside Australia with certain exceptions.[107] In China, personal financial information collected in China may not be stored, processed, or analysed outside China,[108] and similar provisions exist limiting the transfer of personal data,[109] and any data that is deemed to contain a state secret.[110] In India, sensitive personal data or information cannot be transferred abroad unless it is 'necessary' or unless the data subject consents.[111] Russia has comprehensive data localisation rules that require email and social networking companies to retain the data of Russian clients on servers inside Russia, where they can be subject to domestic search warrants.[112] Websites that fail to retain the data in the prescribed manner can be placed on Roskomnadzor's blacklist of websites. Other jurisdictions, such as the EU, are relaxing and even opposing national data localisation requirements as they are considered hindering the free flow of data. Within regulated industries, the lifting of a national data localisation requirement should be replaced with a right of the relevant regulator to 'follow the data' and exercise its supervision even on data being stored outside the borders.

Data localisation measures, while purportedly ensuring domestic access, can create issues for cybersecurity and fundamental rights. By requiring companies to store their data within a particular jurisdiction there is a risk that the companies will not be able to apply the same level of security standards due to the additional obligations (eg, constraints on encryption) placed on them under law. Companies may not be able to achieve the same level of protections they typically apply to their own data centres due to ambiguities within the law. For example, the Russian data localisation regime requires that companies are able to readily distinguish data that relates to Russian citizens from that which does not, a requirement that is difficult for companies to achieve in practice.[113] Furthermore, centralising the data within a given location can diminish overall data security. Local data stores may not apply the same standards as global providers due to limitations on financial resources, less available expertise, or the presence of technological restrictions.[114] Fundamental rights issues may be triggered by these measures as well. Data localisation measures provide a large repository of information that can be accessed. If these measures are enacted, particularly in authoritarian states, there is a greater risk that the information will be accessed and used in a manner contrary to fundamental rights standards. In such instances, data localisation laws may put domestic businesses under pressure to store data in a manner that permits them to circumvent legal protections.[115] If democratic states cite data localisation as necessary, there will be an incentive for

106 Anupam Chander and Uyen P Le, 'Data Nationalism' (2015) 64 *Emory L J* 677, 680.

107 Personally Controlled Electronic Health Records Act 2012 s 77 (Austral).

108 Notice on Urging Banking Financial Institutions to Do a Good Job in Protecting Personal Financial Information] (promulgated by the People's Bank of China, 21 January 2011) (China).

109 Provisions on Protecting the Personal Information of Telecommunications and Internet Users] (promulgated by the Ministry of Indus & Info Tech 16 July 2013, effective, 1 September 2013).

110 Tom Antisdel and Tarek Ghalayini, 'The Challenge of Conducting Data Collections and Investigations Under Unclear Data Privacy Rules', *China Bus Rev*, Oct–Dec 2011, at 46, 48, www.chinabusinessreview.com/the-challenge-of-conducting-data-collections-and-investigations-under-unclear-data-privacy-rules accessed 21 July 2020.

111 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (India).

112 Federal Law of the Russian Federation, 'On Amendments to Certain Legislative Acts of the Russian Federation Regarding the Clarification of the Processing of Personal Data in Information and Telecommunication Networks', *Rosstiskaia Gazeta* 23 July 2014, No 242, available at https://pd.rkn.gov.ru/authority/p146/p191/ accessed 21 July 2020.

113 Federal Law No 242-FZ of July 21, 2014 On Amending Some Legislative Acts Of The Russian Federation In As Much As It Concerns Updating The Procedure For Personal Data Processing In Information-Telecommunication Networks.

114 Erica Fraser, 'Data Localisation and the Balkanisation of the Internet' (2016) 13(3) SCRIPTed 359 https://script-ed.org/?p=3185 accessed 22 August 2018.

115 Large global businesses are better placed to resist such obligations and are more likely to act in a transparent manner to provide information to data subjects on disclosure demands. This may mitigate the risk of data localisation in many instances, but a risk to individual rights remains.

authoritarian states to do so as well. Rather than imposing data localisation obligations, states should permit companies to store their data freely and seek access through other legal mechanisms.

In addition to seeking to apply extraterritorial effect to domestic measures or mandating data localisation, states can seek access to data through international instruments, including, for example, multilateral conventions, bilateral agreements and treaties – through which competent authorities of a jurisdiction may request that other jurisdictions provide judicial assistance and cooperation in relation to civil or criminal procedures.[116] Since 2001, EU Member States have been cooperating increasingly through instruments applying the principle of mutual recognition, on the basis of which the judicial authorities of a Member State recognise the validity of decisions taken by judicial authorities of another Member State.[117] However, while such instruments may facilitate judicial procedures among few states, the lack of international agreements regulating access to information stored abroad may lead to lengthy bureaucratic procedures to force disclosure. The limitations of the current system and recommendations to address the issue are discussed in Chapter XI below.

116 For instance, within the EU the Council adopted the 'Mutual assistance in criminal matters between Member States', a Convention to facilitate mutual judicial assistance between the authorities of the Member States aimed at improving the speed and efficiency of judicial cooperation. The 'Agreement with the United States on mutual legal assistance' sets out conditions relating to the provision of mutual legal assistance in criminal matters between the EU and the US. See: Council Act of 29 May 2000 establishing in accordance with Art 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (2000) OJ C 297 and Decision 2003/516/EC of 6 June 2003 concerning the signature of the Agreements between the European Union and the United States of America on extradition and mutual legal assistance in criminal matters [2003] OJ L181.

117 Examples of mutual recognition in criminal matters in the EU are the European Arrest Warrant and the European Investigation Order. In particular, the latter has the purpose of making cross-border investigations faster and more efficient and covers almost all investigative measures – from the freezing of evidence to the transfer of existing evidence – for Member States participating. See Valsamis Mitsilegas, 'The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU' (2006) 43 *Common Market L R* 1277 www.biicl.org/files/3190_cmlr_mutual_recognition_article.pdf accessed 21 July 2020; European Commission, 'As of today the "European Investigation Order" will help authorities to fight crime and terrorism' (European Commission, 22 May 2017) http://europa.eu/rapid/press-release_IP-17-1388_en.htm accessed 21 July 2020; and Emilio De Capitani and Steve Peers, 'The European Investigation Order: A new approach to mutual recognition in criminal matters' (EU Law Analysis, 23 May 2014) http://eulawanalysis.blogspot.co.uk/2014/05/the-european-investigation-order-new.html accessed 21 July 2020.

Chapter 7: Who should balance rights and interests?

In order to ensure the measures undertaken to guarantee government access do not represent a disproportionate interference with fundamental rights, oversight and accountability mechanisms must be enshrined in the process. An example of an oversight mechanism is the requirement of prior independent administrative or judicial scrutiny before access is permitted.[118] Balance between the different interests may be achieved by requiring governments to obtain an authorisation in order to access to data on IT systems. This is particularly common in the context of criminal investigations, where the obtainment of certain data could be crucial as evidence. In particular, domestic laws may require the obtaining of:

- Warrants – for example in the US, under Section 2703 of the US Stored Communication Act (SCA), a governmental entity may require a provider of remote computing service to disclose the content of any wire or electronic communication, without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure or in the case of state court, using the state warrant procedures, by a court of competent jurisdiction;

- Judicial requests – under Australian law, for example, one of the key exceptions to the protections afforded to individuals under the Privacy Act in relation to the disclosure of their personal information is when an act or practice is 'required or authorised by or under law, including court/tribunal orders'. Similarly, the judgment in Digital Rights Ireland held that 'it is essential that access of the competent national authorities to retained data should, as a general rule (except in cases of validly established urgency) be subject to a prior review carried out by a court or by an independent administrative body, and that the decision of the court or body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection, or prosecution of crime';[119] or

- Authorisation by the corresponding administrative body – in this regard, for example, the UK Government has enacted the Data Retention and Acquisition Regulations 2018, which permit the Investigatory Powers Commissioner (IPC) to authorise data access requests for communication data. These powers are delegated to a new body called the Office for Communications Data Authorisation. For urgent requests for access to communications data, a designated senior officer in a public authority (not including local authorities) is permitted to authorise such requests.

However, the requirement to obtain a judicial approval might not be enough to protect individuals. Even with existing laws that require the obtainment of prior court authorisation, governments might still have scope to indiscriminately access individuals' information if such laws are drafted broadly. For instance, in Russia, a ministerial order from the Russian Ministry of Communications introduced requirements for the new wiretapping system SORM-3 (System for Operative Investigative Activities) that allows for interception

118 Council of Europe Convention on Cybercrime art 15 for signature Nov 23, 2001, S TREATY Doc No 108-11 (2006), ETS No 185 (entered into force 1 July 2004).

119 See also Art 22 of the Brazilian Marco Civil, which governs the judicial request to access the records mentioned above. It establishes that an interested party – such as a governmental authority – may, for the purpose of gathering evidence in civil or criminal lawsuits, request in court that the entity responsible for keeping the records disclose them. The judge shall only grant such a request in case the plaintiff is able to (1) demonstrate reasonable evidence of the occurrence of an illicit act; (2) demonstrate the usefulness of the requested records for the investigation or probative instruction; and (3) indicate a specific period of time for the records requested. The judge shall take all necessary measures to ensure the confidentiality of the information received so as to preserve the intimacy, private life, honour and image of the user (Article 23).

of telephone and internet communications in Russia. Typically, to get hold of such communication a court warrant is required, however, the Federal Security Service ('FSB') may start the process in its absence. Such access may be subject to an ex post review in order to satisfy oversight requirements. However, 'retrospective review is likely to be less rigorous than prior scrutiny and it may well be easier to satisfy the requirements of necessity and proportionality when armed with the incriminating results of the surveillance'.[120] Furthermore, under Russian law, a warrant is only a prerequisite for the seizure of content, while metadata – eg, phone numbers of the communicating parties, time, location etc – can be obtained without any obligation to present a warrant to the other party. A lower threshold for metadata, which can be highly revealing in itself, offers insufficient protections for individuals. In order to avoid such practices, domestic laws shall provide clear definitions of 'data', 'personal data', 'government', 'access' etc, and require that wherever possible, independent approval is sought for authorisations prior to access.

In addition, in cases where national security is at stake, governments may not have to go through securing a formal authorisation at all.[121] Although this may be reasonable, it should only happen in specific circumstances due to their nature and should be applied very cautiously in specific circumstances so as not to incur any abuse of law.[122]

Abuse and misuse of power by governments may be – at least partially – avoided if the provisions contained in domestic laws are clear rather than vague and subject to interpretation. However, recognising that a provision that is clear and immune from the need for interpretation may prove to be inflexible or frequently inapplicable, some jurisdictions' legislative or regulatory language may adopt a principles-based or outcome-based approach. The judiciary can play a key role in balancing the interests of the different parties as judges apply domestic laws and provide interpretations accordingly.

With reference to targeted access to information, where investigating authorities are required to obtain a court authorisation or warrant before being allowed to formally request and obtain data, the judiciary can act as an independent and autonomous body and balance the different rights/interests and provide adequate legal remedies, taking into account the principle of proportionality and assuring an effective application of the rule of law.[123]

The judiciary may not always have the statutory authority to oversee measures undertaken by state security and intelligence agencies, which may have broad discretionary powers. However, the discretionary power of state agencies, administrative bodies, enforcement authorities or other public bodies should meet certain thresholds. The secrecy of measures that may be needed, for example with intelligence operations, should not set them outside the law, nor prevent them being subject to effective oversight. For such cases, specialist independent tribunals with power to take decisions and enforce the same can be set up

120 Judith Rauhofer, 'Privacy and Surveillance: Legal and Socioeconomic Aspects of State Intrusion into Electronic Communications' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (Hart Publishing 2009) 561.

121 The Australian Security Intelligence Organisation (ASIO) possesses a range of special powers in relation to data gathering for national security purposes, including the power to use listening devices and tracking devices in order obtain intelligence-related information. Under Australian Law, under s 3ZQN of the Crimes Act, if 'an authorised Australian Federal Police (AFP) officer considers on reasonable grounds that a person has documents (including in electronic form) that are relevant to, and will assist, the investigation of a serious terrorism offence', they can access that document by giving written notice requiring the person to produce specific documents, without any prior court approval. See: Crimes Act 1914 (Cth), Part 1AA, Divison 4B (Australia).

122 See n 20 above – a set of laws toughening the previously introduced legislation relative to the data storage and government surveillance. Among others, telecom providers are now obliged to store the content of data images, video calls and text messages for six months and metadata for three years. All social media providers as well as messengers and email clients, that are using data encryption, are mandated to share their encryption key with the FSB. All relevant communication and metadata shall be promptly disclosed to authorities on first demand and without a court order.

123 In his work on the rule of law, Lord Bingham notes that, 'all persons and authorities within the state, whether public or private, should be bound by and entitled to the benefit of laws publicly and prospectively promulgated and publicly administered in the courts'. Tom Bingham, *The Rule of Law* (Penguin 2011) 8.

to ensure effective oversight and balancing of the different interests at play. In addition to providing mechanisms for approval prior to access, either through judicial review or approval by an established independent tribunal, domestic laws should provide limits to the power of the government to access or receive information, in particular when dealing with personal data of the citizens. However, we note that the lawmakers may not have deep technical knowledge of the topic at hand, with reference to the recent development of technologies, how the new IT systems and devices are being used, how the databases are being created and maintained, etc.

In order to be able to enact laws sufficiently and appropriately balance the different rights and interests involved, national legislators should be adequately informed about IT systems, databases and the complex issues related to this specific sector. This may require engaging with academics, experts, private companies and other entities in the IT services industry to acquire a better understanding of the relevant issues. This occurs in the UK, for example, during the legislative process when expert opinions from the private sector, academics and civil liberties organisations are sought prior to the passage of any Acts related to the use of these technologies. After the enactment and enforcement of such laws, there should be monitoring and reporting on the application of the same, followed by an evaluation process to see the effects and identify any further amendments. In this regard there is a growing interest in the creation of 'public advocacy positions' within the authorisation processes. Reports have acknowledged that the technology companies should similarly play a role in authorising access when such access affects their interests and allowing them to challenge existing measures.[124]

124 See n 36 above, para 38.

Chapter 8: Transparency regarding access

In case of government access to personal data collected and stored by a private entity, several obligations exist in relation to the obligation to assure proper use and security of the data acquired. Such obligations may include, for example, notification and responsibility for damages if access is given in excess of permission. For example, in the UK, if an error occurs in obtaining or disclosing the data, that error must be reported to the IPC who oversees access to data by public authorities. If that error is deemed 'serious' under section 231 of the Investigatory Powers Act, the IPC is entitled to inform individuals of serious relevant errors in the use of investigatory powers that relates to them. Here a relevant error is 'an error made by a public authority in complying with any requirement over which the Investigatory Powers Commissioner has oversight'.[125] This provision remains a power that may be exercised rather than a mandatory requirement. The right to inform an individual is limited to those instances where it is both in the public interest to inform the individual, and significant prejudice or harm to the person concerned has resulted.[126] It is for the IPC to undertake an examination of the error and balance the seriousness against the public interest in non-disclosure. This is a discretionary power; there are no binding or determinative requirements for conduct that will amount to 'serious'. If the affected individual so choses, upon being informed that a 'serious error' has occurred with regard to his or her data, they may challenge the legitimacy of the action before the Investigatory Powers Tribunal.

The ability to bring an action before a court to seek remedy is crucial to ensuring the interference occasioned by the actions of public authorities is done in accordance with the rule of law. In order to adequately avail themselves of the right to seek a remedy, there may be an obligation on states to inform individuals that their data has been accessed. It was held in the case of *Tele2* and *Watson* that 'the competent national authorities to whom access to the retained data has been granted must notify the persons affected… as soon as that notification is no longer likely to jeopardise the investigations being undertaken by those authorities. Notification is necessary to enable to persons affected to exercise, inter alia, their right to a legal remedy'.[127] Notification is supported by bodies such as the UN[128] and the Venice Commission,[129] who reiterate the necessity of notification for individuals who have been subjected to actions by public authorities.

Government access should be transparent and regulated. Whenever the public investigation authorities process – directly or indirectly – an individual's personal data suspecting them of involvement in a serious crime, the individual should be informed of such processing unless there are reasonable grounds

125 Explanatory Notes to the IPA para 643.

126 *Ibid*, para 644.

127 Joined Cases C-203/15 *Tele2 v Post-och telestyrelsen* & C-698/15 *Watson & Ors v Secretary of State for the Home Department* (2016) ECLI 970 para 121; Case C-362/14 *Max Schrems v Data Protection Commissioner* (2015) OJ C351/14 para 95; *Weber & Saravia v Germany* App no (54394/00) ECHR 29 June 2006 para 135; Case C-553/07 Rijkeboer [2009] EU:C:293 para 52; *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 4 Dec 2015) para 287; and *Szabo & Vissy v Hungary* App no 37138/14 (ECtHR, 12 Jan 2016) para 86. However, this precedent seems to directly conflict with the ruling in Klass & Ors v Germany App no 5029/71 (ECtHR, 6 Sept 1978) where it was held that 'In the Court's view, in so far as the "interference" resulting from the contested legislation is in principle justified under Art 8 para 2, the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision since it is this very fact which ensures the efficacy of the "interference"', para 58.

128 See the report of United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, which found that: 'individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the state', para 82, 2013 ['Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (UN 2013) A/HRD/23/40].

129 'Individuals who allege wrongdoing by the State in other fields routinely have a right of action for damages before the courts. The effectiveness of this right depends, however, on the knowledge of the individual of the alleged wrongful act, and proof to the satisfaction of the courts.' See: Venice Commission, 'Report on the Democratic Oversight of the Security Services' Study no 388/2006 (CDL-AD(2007)016).

to believe that this will prejudice the investigation. In case of data processing as part of surveillance operations and the protection of national security, transparency is often difficult to organise from a practical perspective and/or undesirable to avoid undermining the effectiveness of a programme. In such case, upfront clearance of a surveillance programme in combination with strict guidelines, oversight and post-factum transparency (eg, notifying a suspect that certain data will be used as part of a prosecution) can provide acceptable alternatives. Furthermore, should any person suffer material or non-material damage due to an 'unreasonable' or 'unjustified' violation of their right to privacy by the government, the individual should have the right to a remedy. This provision is enshrined in human rights instruments such as Article 13 of the ECHR. The remedy may take the form of data deletion, an order for access being quashed, or potentially compensation for the damage suffered.

Chapter 9: Position of electronic communications service providers

Due to their role as providers of IT systems that collect and store vast amount of information, it is necessary to examine the position of service providers. The electronic communications service providers (CSPs) are often sought out by authorities and investigators to act as facilitators for access, providing the basic necessary infrastructure to be able to disclose the required information. In this regard, service providers act as a forced conduit; information is collected and retained on their system and, in the same manner and form, it is passed on to investigators. The delegation of this power to private entities has a considerable impact on the traditional norms associated with access. Notably, there exist immunities for companies who comply with legitimate access requests.[130] 'As a result, these companies are subject to neither the burden of transparency nor the constitutional constraints imposed upon state actors'.[131] While the legal onus for transparency is only binding on public authorities, companies often act as key advocates for transparent access processes. This includes taking actions that range from publishing information about access requests to challenging the right of governments to access their data before the courts. Liability for companies in the access process is limited; information that is incorrect or shared erroneously will not usually give rise to legal responsibility. The requirement that CSPs act as facilitators here can enable the subversion of traditional protections concerning access. Typically, a public body will be limited in the manner in which it can search through electronic information. By requiring CSPs to do this, traditional limitations and protections for fundamental rights can be more easily avoided.[132]

In addition to the implications for fundamental rights that arise in complying with data access requests, service providers may be impacted in other ways as well. Commercial interests may also be affected by the attempt of governments to access certain data. This is the case of many service providers (eg, internet application providers)[133] or owners of digital platforms, which may reject government access due to various corporate concerns, including ownership and intellectual property rights, confidentiality agreements, impact on innovation, company reputation, consent of the customers, client retention, and the associated costs of compliance. If the company is required to process the data to meet a request, there must also be measures in place for the company to receive compensation for the action.[134] Financial interests are triggered by any requests for access. There is the possibility that such requests, if disclosed to the end users of a service, may decrease the trust consumers have in the technology companies. Further, any provisions that mandate the inclusion of access capabilities will have implications for the global competitiveness of service providers. This is particularly significant due to the global nature of communications and

130 In the US, the FISA Amendments Act 2008 HR 6304 granted retrospective immunity from civil liability to telecommunications companies engaged in warrantless domestic surveillance activities. Federal Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub L No 110-261, ss ss 702(h)(3), 703(e), 122 Stat 2436 (2008).

131 Nancy S Kim and D A Jeremy Telman, 'Internet Giants as Quasi-Governmental Actors and the Limits of Contractual Consent' (2015) 80 *Mo L R* 723, 745; This is also the case in the US where the Foreign Intelligence Surveillance Act offers immunity from breach of contract claims when they share information with the government in violation of privacy provisions in their agreements with customers [Federal Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub L No 110-261, ss ss 702(h)(3), 703(e), 122 Stat 2436 (2008)].

132 Niva Elkin-Koren and Eldar Haber, 'Governance by Proxy: Cyber Challenged to Civil Liberties' (2016) 82 *Brooklyn L R* 105, 107.

133 Art 13 of the Brazilian Civil Rights Framework for the Internet (Law No 12,965/2014 or 'Marco Civil') states that internet connection providers must maintain users' connection records under confidentiality for one year. Authorities do not have the power to access them without a judicial order. Furthermore, the Marco Civil establishes that internet application providers must keep application access records under confidentiality and in a safe environment for six months. The disclosure of such records also depends on a court order (Art 15). While providing users with internet applications, a company is prohibited from retaining the records of access to other internet applications without users' prior and express consent. In addition, such company cannot collect personal data that is not related to the purpose for which the consent was given in first place by the owner of the data (Art 16).

134 This is provided for in the Investigatory Powers Act 2016 ss249(1) and (2) (UK).

the international market in which modern technology companies operate. Any measures which oblige companies to retain data can pose a threat to the global competitiveness of these companies if it is later disclosed that governments have been obtaining access to the data unbeknown to users. In this regard, US technology companies, for instance, have already begun losing business with foreign customers due to persistent data access requests by US law enforcement agencies. For example, in 2014 the German government cancelled a contract with Verizon – a US telecoms company that has provided internet services to a number of German government departments – over concern that US firms may be giving data to US authorities.[135]

Consequently, any measures that require service providers to permit access to the data they generate and collect must meet acceptable standards and be clearly provided for by law. Typically, companies now require data requests to go through legal channels before they will permit access to their systems.[136] The access provided will be limited based on what data is needed. Where the law is ambiguous as to what level of process is required, companies may demand that a higher level of process is met.[137] Companies can utilise techniques of proceduralism and litigiousness to ensure any access requests are strictly confined. The ability of companies to challenge any access request or demand that it meets certain standards is significant. Companies may be the only entities with the standing to challenge a request.[138]

In addition to requiring governments to comply with domestic law in gaining access to data, service providers also play a significant role in securing the data. Service providers' design decisions can make government access more difficult.[139] This can occur through a variety of technical means, such as encryption. Security measures applied to the communications or data render it impossible to access without further information, such as encryption keys, being provided. Other technical means that frustrate access include choices by companies as to what type of data to retain. If the company chooses not to store the categories of data that law enforcement seeks, then access cannot be given, and other mechanisms will need to be applied. Furthermore, as a commentator explains, companies 'may simply fail to create the capabilities or invest the resources needed to respond […] quickly or at all'.[140] Through developing their technical infrastructure, service providers can exercise control over access to their data.

The desire to protect their consumers from unwarranted access is evident in publicised policies of service providers. For example, on 27 January 2014, global technology and security companies – including Microsoft, Google, Facebook, LinkedIn, Apple, Twitter and Dropbox, among others – formed a coalition to pressure governments into reassuring their customers about the legality of their data sharing and access procedures.[141] The Reform Government Surveillance coalition set forth principles for governments to

---

135 'Germany cancels Verizon contract over snooping fear' BBC (26 June 2014) www.bbc.co.uk/news/business-28047877 accessed 8 September 2018.

136 There are exceptions to this, for example, where voluntary arrangements are agreed between the service providers and the government. One such provision is under the Stored Communications Act (SCA) in the United States, which permits the voluntary disclosure of communications content if the provider, in good faith, believes that an emergency involving danger of death or other serious physical injury to the person requires disclosure without delay [Stored Communications Act 18 USC ss2702(b)(8)].

137 See *United States v Warshak* 631 F 3d 266.288 (6th Cir 2010). In this case the precedent was set that warrants were required to disclose the content of emails under the Stored Communications Act, even if the statute permitted lesser process.

138 This is the case in the US wherein *Clapper v Amnesty International* established that plaintiffs could not establish standing to challenge surveillance programmes absent concrete knowledge that they were targets of the surveillance. This is not the case in the UK however where the court has acknowledged that applicants may challenge a measure on the basis of assumed facts [Investigatory Powers Tribunal Rules 2000, SI 2000/2665, 2.8].

139 This occurred in the *Apple v FBI* case wherein Apple had recently updated its iOS against third-party access, including that of Apple itself. [See Memorandum of Points and Authorities at 1-4, In re Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, No. ED 15- 0451M, 2016 WL 618401 (C D Cal Feb 16, 2016), 2016 WL 680288].

140 Alan Rozenshtein, 'Surveillance Intermediaries' (2018) 70 Stan L R 99, 139.

141 Spencer Ackerman, 'Tech giants reach White House deal on NSA surveillance of customer data' *The Guardian* (Washington, 27 January 2014) www.theguardian.com/world/2014/jan/27/tech-giants-white-house-deal-surveillance-customer-data accessed 24 August 2018.

adhere to when conducting surveillance. According to these principles, the companies stress the need for policies to:

- limit government ability to collect users' information, stressing that the interest in data must be balanced against privacy interest and impact on trust in the internet; and
- 'allow companies to publish the number and nature of government demands for user information. In addition, governments should also promptly disclose data publicly'.[142]

The companies in the coalition advocate for legal reforms that would ensure government access to data is consistent with established global norms and the rule of law.

Where a public authority – such as government, the FBI, judges or courts – requires a private firm to provide access to data, the company is obligated to comply provided the request meets the requirements of local legislation. Thus, in front of a request or warrant issued by public authorities, all is in the power of the above-mentioned companies to object and take the case to court. However, where no legal protection is provided – such as the metadata case in Russia – service providers may have no other choice but to comply with the request.

In addition, it is important to acknowledge the growing prevalence of providers of OTT services (as, for example, Skype, Netflix etc). These OTT services are becoming dominant modes of communication and are increasingly subject to data retention and access obligations.[143] Domestic provisions, such as the Investigatory Powers Act in the UK, make it clear that the requirements therein are meant to apply to OTT providers as well as more traditional telecommunications services. Moreover, while in some cases decoding messages sent through OTT services may require only the cooperation of telecommunications service providers, in other cases governments may need help from the OTT providers themselves. In this regard, it is important that OTT providers are subject to the same oversight and safeguards provided to traditional service providers. There should in principle be no loophole for government access by virtue of a distinction between an OTT and a telecom provider.

At the same time, due regard should be given to the fact that OTT providers do not have the same measure of technical control over the underlying infrastructure (eg, the internet) as the telecommunications service providers may have over their own backbones. As a result, certain obligations for OTT providers need to relax to accommodate this constraint. This is how the new European Code for Electronic Communications came to consider the OTT providers as a specific subset of providers of electronic communication services, that is as providers of Interpersonal Communication Services (ICS), with corresponding obligations.

Furthermore, service providers may offer an element of transparency concerning access to data by publishing relevant reports. Many large technology companies, such as Google and Facebook, publish statistics on how many government access requests they receive. These reports are becoming an industry standard. Through the publication of this information, the companies involved in the access process

142 Global Government Surveillance Reform: The Principles (2013) available at: www.reformgovernmentsurveillance.com/principles accessed 19 August 2019.

143 Body of European Regulators for Electronic Communications, 'BEREC Report on OTT services', 2016, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services accessed 19 August 2019.

provide information through which the public can learn about government access. Tensions have arisen where governments have imposed limitations on the level of granularity of the transparency reports.

The role of the service providers in the access regime is crucial. Companies should consider the potential implications of access, not just for their commercial interests, but for fundamental rights standards as well. In order to ensure these companies support fundamental rights, due regard should be had for any access requests that potentially place these rights at risk. In particular, due regard should be had for the UN Guiding Principles on Business and Human Rights to ensure companies meet these standards when complying with access requests as provided for by law.[144]

144 OHCHR, Guiding Principles on Business and Human Rights (2011) www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf accessed 12 August 2018.

Chapter 10: Towards an international legal framework

Governmental access is a worldwide issue that presents an international challenge to privacy. In cases of cross-border access, interests and rights of other states are relevant, particularly in terms of territorial jurisdiction and sovereignty. The complex issues herein demonstrate the need for new mechanisms to facilitate cross-border access to data while also respecting sovereign interests in protecting privacy.

The current legislative framework that provides for access to data across jurisdictions relies on Mutual Legal Assistance Treaties (MLATs), which can be slow and laborious. The length of time it takes to gain access through the MLAT system has led governments to request the data directly from companies rather than going through the legal process. The US, wherein the majority of relevant technology firms are based, can take an average of ten months to respond to requests made pursuant to an MLAT.[145] The length of time the process takes renders the measures ineffective for the prompt investigation of crimes and determination of national security threats. Further, there is a lack of transparency throughout the MLAT process. Requesting officials are often unable to determine who is handling their requests, the length it will take for the request to be answered, and any mechanisms to challenge a decision.[146] The difficulties are further exacerbated by gaps in the process, as not every country is subject to a MLAT.

In the recent past, several cases demonstrated failings with the MLAT process and emphasised the need to introduce international instruments in relation to the topic at hand. For instance, as part of the investigation into a drug-trafficking case, in 2013 a federal magistrate's court in New York granted a search warrant to the Department of Justice (DoJ) under the SCA[147] requiring Microsoft Corporation to produce emails and personal user data associated with an account they hosted. The multinational tech company provided the requested account information – which was held on US servers – but refused to turn over the emails as the latter were stored at a data centre located in Dublin. Microsoft argued that the data it held on Irish servers was not subject to US jurisdiction and, thus, challenged the warrant.[148] Since the US signed a MLAT with Ireland, the company held that the US law enforcement should use the MLAT and go through the Irish authorities to obtain the emails.[149] However, the federal magistrate and then the District Court judge subsequently held that the SCA warrants are not restricted by territorial constraints and ordered the company to retrieve the customer's correspondence from Ireland and provide it to the government. Microsoft appealed to the Second Circuit Court of Appeals in New York, which in 2016 stated that the Congress, in enacting the SCA, did not expressly provide for extraterritorial reach. In response, the DoJ appealed to the Supreme Court, which decided to hear the appeal. However, in the meantime, in March 2018 the US passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which created new procedures for procuring legal orders for data in cross-border cases as the one discussed here. Therefore, the DoJ withdrew the warrant that was at the centre of the dispute and procured a new warrant

145 See n 102 above, 393.

146 Andrew K Woods, 'Data Beyond Borders: Mutual Legal Assistance in the Internet Age' (Global Network Initiative 2015) 3 https://perma.cc/PA6M-XVLZ accessed 20 July 2020.

147 The warrant was issued under Stored Communications Act (US) 18 USC ss2703.

148 *United States v Microsoft Corp.*, 584 US _ (2018).

149 Louise Matsakis, 'Microsoft's Supreme Court Case has Big Implications for Data' (Wired, 27 February 2018) www.wired.com/story/us-vs-microsoft-supreme-court-case-data accessed 22 August 2019.

under the CLOUD Act.[150] The US Government moved to drop the lawsuit and in April 2018 Microsoft agreed that the new law rendered the lawsuit moot.[151]

In another case, similar to the above, the US judiciary reached a different conclusion. In 2017, as part of a domestic fraud investigation, Google was requested to comply with a warrant and hand over the emails of Gmail users stored outside the US. The ruling at hand came less than seven months after the Second Circuit Court of Appeals ruled Microsoft could not be forced to turn over emails stored on a server in Dublin. Even though both cases involved warrants issued under the SCA and were similar, the magistrate in this case departed from precedent as – due to the fact that Google's system partitions user data into shards – it is difficult to establish which foreign country's sovereignty would be implicated when the company accesses the communications to produce it in response to a legal process. On the basis of such statement, it seems that the use of Legal Assistance Treaties requires a territorial link.[152]

In two Belgian cases, the Supreme Court allowed a local investigating magistrate to determine jurisdiction over Yahoo Inc in the US, and Skype in Luxembourg, to compel the production of data in the first case and the installation of a wiretap in the second case. In both cases, jurisdiction was in essence assessed based on the fact that the results of the measure were to be used for the purpose of a criminal investigation taking place in Belgium.[153]

As governments face potential limitations on their access to data, further measures are proposed and/or enacted to ensure access remains. These remain piecemeal, varying across jurisdictions, and are unlikely to address the failings that exist under the MLAT system. However, it is worth discussing some of these developments here.

In Brazil, a Data Protection Act (Lei Geral de Proteção de Dados) has been enacted and will come into effect in August 2020. Under the Act, the law will have extraterritorial scope, applying to companies that process data relating to Brazilian domiciled individuals.[154] Provisions are included that permit international data transfers to foreign jurisdictions provided the transfer is necessary for international legal cooperation between intelligence, investigative or prosecutorial agencies.

The CLOUD Act – already mentioned in relation to the case *Microsoft v US*, provides for the execution of new types of international agreements allowing foreign governments to access data held by US providers. Nevertheless, for a country to qualify for such an agreement with US authorities, the US Attorney-General must first certify that the country's legal environment provides certain legal protections, such as defending privacy and civil liberties.

To strengthen cross-border cooperation in investigations, on 17 April 2018 the European Commission proposed a legislative package composed of a regulation and a directive allowing EU Member State authorities to access – directly from services providers – electronic evidence held outside the European

150 Sarah Jeong, 'The Supreme Court fight over Microsoft's foreign servers is over' (The Verge, 5 April 2018) www.theverge.com/2018/4/5/17203630/us-v-microsoft-scotus-doj-ireland-ruling accessed 22 August 2019.

151 See n 148 above.

152 John Ribeiro, 'Google ordered by US court to produce emails stored abroad' (PC World 6 Feb 2017) www.pcworld.com/article/3165869/internet/google-ordered-by-us-court-to-produce-emails-stored-abroad.html accessed 27 August 2018; Samuel Gibbs, 'Google to appeal against order to hand over user emails stored outside US' The Guardian (6 February 2017) www.theguardian.com/technology/2017/feb/06/google-gmail-to-appeal-against-order-to-hand-over-user-emails-stored-outside-us accessed 27 August 2018.

153 See n 101 above.

154 Brazilian General Data Protection Law (LGPD), Federal Law no 13,709/2018.

Union or in another EU Member State.[155] In fact, according to the proposal, judges, courts, investigating judges, as well as other investigating authorities in criminal proceedings with competence to order the gathering of evidence in a Member State, may order a service provider offering services in the EU to produce or preserve electronic evidence. The orders – called 'European Production Order' and 'European Preservation Order' respectively – shall be used only in cross-border situations, in particular when the service provider is established or represented in another Member State. Moreover, the proposal – if adopted by the EU Parliament and the Council – will be applicable to service providers in the EU and to the representatives of providers outside the EU offering within the EU:

- electronic communications services;
- information society services that store data, such as social networks, online marketplaces and cloud providers; and
- internet domain name and IP numbering services, such as IP address providers, and domain name registries.

In addition, on the basis of the draft of the Regulation, data storage is usually determined by the provider alone, and the state on whose territory data is stored has no control over such data. The draft moves away from data location as a determining factor and, therefore, the above-mentioned judicial and investigating authorities may request that companies provide/preserve:

- subscriber data (eg, date of birth, postal or geographic address, telephone or email);
- access data (eg, date and time of the service, log-in/off from the service or IP addresses);
- content data (eg, text or voice messages, images/videos); and
- transactional data (eg, data on the location of the device, date, time, duration, route or the protocol used), regardless of where such data is located.

Furthermore, attention should be given to the EU proposal of the e-Privacy Regulation. On 10 January 2017, the European Commission (EC) published a new proposal for an e-privacy Regulation that will replace the e-Privacy Directive. As a regulation, it is expected that it will be directly applicable to all Member States. The scope of the Regulation has been extended to apply to any company processing personal data in the context of delivering electronic communications and files, including so-called OTT providers like Gmail, WhatsApp and Netflix. According to Article 5, all electronic communications data must be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end users, is prohibited.

Article 6 of the proposed Regulation also specifies when processing of electronic communications data, metadata and content is exceptionally permitted and/or needs the consent of the user. Article 7 addresses storage and erasure of electronic communications data and Article 8, the protection of information stored in and related to end users' terminal equipment. Article 11 foresees that Union or Member State

155 Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters' COM (2018) 225 final; and Commission, 'Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' COM (2018) 226 final.

law may restrict by way of a legislative measure the scope of the above obligations and rights where such a restriction (1) respects the essence of the fundamental rights and freedoms, and (2) is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests listed in Article 23(1)(a) to (e) of the General Data Protection Regulation (GDPR) (ie, national security, defence, public security, prevention, investigation or prosecution of criminal offences or the execution of criminal penalties, and 'her important objectives of general interests', which include taxation, social security and health) or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests. With regard to the GDPR, the current provisions require that for any data being transferred on the basis of a request for access from a non-EU country, there must exist an international agreement such as an MLAT in force between the requesting party and the Member State.[156]

However, despite these new and proposed legislative acts, problems remain with utilising the existing mechanisms of international agreements and MLATs to provide access to data across jurisdictions. It is therefore suggested that steps should be taken to create an international framework to govern cross-border information exchanges.[157] One potential model for this that has been suggested is the European Convention on Cybercrime (commonly known as the Budapest Convention). In its current form, this provides a mechanism for nations to expedite and facilitate cross-border sharing of information relating to cybercrime.[158] This mechanism may be extended to sharing information for other criminal matters as well. The Budapest Convention has been ratified by over 44 countries, including EU Member States as well as Australia, Japan, Mauritius, Panama and the US. Under this Convention, states are required not only to cooperate with each other in accordance with relevant international instruments for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data,[159] but to ensure in so doing they comply with relevant human rights obligations. To that end, any use of the powers under the Convention must provide for the adequate protection of human rights pursuant to obligations under the ECHR and ICCPR which mandate that the provisions be legitimate, necessary and proportionate. In addition, the powers are to be utilised in accordance with acceptable safeguards, including judicial or other independent supervision and limitations on the scope and duration of the powers.[160]

Other proposals for international legal frameworks governing access to data have similarly been posited by relevant stakeholders. Brad Smith of Microsoft has called for an international convention on government access to create surveillance and data access rules across borders.[161] This convention would similarly place respect for human rights and privacy as the cornerstone of any access regime. This convention would create new processes to supplement the existing MLAT rules.[162] Other proposals suggest relying on principles of 'bilateral parity' wherein requests for access would be streamlined between states that agreed

156 General Data Protection Regulation 2016/679 Art 48.

157 Such provisions do currently exist with regard to remote sensing data in outer space. The Principles relating to remote sensing of the earth from outer space (Remote Sensing Principle) UNGA 41st Session 1986 entitled the sensed state to have access to the primary (unprocessed) and processed data concerning its territory on a non-discriminatory basis and to the analysed information resulting from remote sensing data in the possession of any state participating in the remote sensing activities on the same basis and terms.

158 Council of Europe Convention on Cybercrime arts 17-18, 32, opened for signature Nov 23, 2001, S TREATY Doc No 108-11 (2006), ETS No 185 (entered into force July 1, 2004).

159 *Ibid*, Art 23.

160 *Ibid*, Art 15.

161 Brad Smith, 'Time for an international convention on government access to data' (Digital Constitution 20 January 2014) https://perma.cc/W8J3-YYVG accessed 19 August 2018.

162 *Ibid.*

to apply similar protections and legal processes to data.[163] Such provisions would permit the sharing of data or granting of access to countries that guarantee they will provide other states' citizens the same rights as their own.[164] Several sets of principles have been agreed to by some relevant stakeholders involved in the access process. The so-called 'necessary and proportionate' principles set out 13 principles that aim to codify and apply human rights obligations to communications surveillance.[165] Thus far the principles have been endorsed by over 600 organisations. The 'Company Principles' similarly dictate five principles for surveillance reform and are endorsed by the global tech giants, including Microsoft, Facebook, Apple and Google.[166] These recommendations call for an end to bulk collection of data, enhanced disclosure of the legal authorities that require disclosure, increased transparency and better oversight of the agencies involved in the processes.

Recent reports at the international level have similarly called for a unified international framework and consistent application of human rights principles to data accessed by governments. In the Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression issued by the Special Rapporteurs of the UN and Inter-American Commission on Human Rights, the need for limited access under only exceptional circumstances was stressed. The Declaration similarly noted the need for the access to be confined in scope and duration, subject to independent or judicial oversight, and protected by due process guarantees.[167] Further reports from the High Commissioner for Human Rights and the Special Rapporteur on counter-terrorism and human rights have stressed the need for further scrutiny of these powers.[168]

All in all, there is a common concern regarding access to data by governments. Any recommendations for reform should address the common concerns which arise across jurisdictions, as it is no longer possible to treat access to IT systems as a singular country issue. The principles discussed below represent best practice in prescribing an overarching international legal framework to apply to government access to IT systems.

163 Kate Westmoreland, 'A New International Convention on International Legal Cooperation?' (ACS Blog 2 September 2015) (American Constitution Society) https://perma.cc/3ZMB-YL56 19 August 2018.

164 Stephen J Schulhofer, An International Right to Privacy? Be Careful What You Wish for 26 (NY *Univ Pub Law & Legal Theory*, Working Paper No 508, 2015), https://academic.oup.com/icon/article/14/1/238/2526788 accessed 21 July 2020. .

165 The International Principles on the Application of Human Rights to Communications Surveillance (the 'Necessary and Proportionate Principles') (2013) https://necessaryandproportionate.org accessed 21 July 2020.

166 See n 142 above.

167 Joint Declaration on Surveillance Programs and their impact on Freedom of Expression, issued by the UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (June 2013) paras 8 and 9.

168 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, A/69/397 (23 September 2014) para 12.

Chapter 11: Access to data held or generated by lawyers

The effective protection of society from potential threats deriving from the abuse of power depends on – inter alia – the existence of a system of checks and balances. In fact, it is universally acknowledged that the separation of powers between the legislature, the executive and the judiciary is one of the fundamental principles of a democratic society.

There is no liberty if the judiciary power is not separated from the legislative and executive. Were it joined with the legislative, the life and liberty of the subject would be exposed to arbitrary control, as the judge would be then the legislator. Were it joined to the executive power, the judge might behave with violence and oppression.[169]

The autonomy of judicial power entails the independence of judges, prosecutors and lawyers. In particular, it is highlighted that an independent legal profession is necessary in order to enable lawyers to effectively assist and protect citizens' legitimate rights against public powers and private parties. In fact, such independence enables lawyers to act in the legitimate interest of their clients – but also society as a whole – without fear of abusive prosecution and free from improper interference or influence of any kind.[170]

Attorney–client confidentiality is the key element in establishing and securing an effective fiduciary trust between the client and the lawyer in the legal profession. New legislation granting governments further powers to access confidential client information covered by professional privilege/secrecy represent a serious threat to lawyers' ability to properly perform their function and protect their clients' interest without external interference. Further concerns are related to the effective protection of the client's right to a fair trial, including the right to adequately prepare a defence. Moreover, the possibility of disclosure may also undermine the fiduciary relationship between lawyers and their clients, in particular where a prior consent of the client is not required.

Due to the increasing use of emails and internet in the communication between lawyers and clients, government surveillance – and, in particular, indiscriminate mass surveillance – may represent a risk for professional secrecy. Information that once would have been kept under lock in the lawyer's office is now transmitted through electronic means and stored in a computer memory or the cloud. Therefore, such confidential information – in the form of electronic data – may be anywhere in the world and is vulnerable to interception, use and disclosure by security agencies of the home state, but also foreign powers.

Information may be kept by the lawyers in different forms – as hard copies, data saved on mobile devices such as smartphones, or on laptops or desktops in lawyers' offices, as well as electronic data stored in the cloud. In each form, it shall be covered by professional secrecy and protected under law from any violation. As for search and seizure in a law office, in most European countries the investigating authorities are required to obtain a court warrant/authorisation before proceeding. Additionally, there is a requirement of prior permission from the prosecutor or a prior notification of the Bar regulating the

169 Charles de Secondat, Baron de Montesquieu, 'The Spirit of Laws', *Complete Works* (vol 1, book XI, 1748) http://oll.libertyfund.org/titles/montesquieu-complete-works-vol-1-the-spirit-of-laws accessed 21 August 2018.

170 Office of the High Commissioner for Human Rights in cooperation with the International Bar Association, 'Human Rights in the Administration of Justice: A Manual on Human Rights for Judges, Prosecutors and Lawyers', professional training series no 9, 2003: www.ohchr.org/Documents/Publications/training9chapter4en.pdf accessed 22 July 2020.

lawyer. Furthermore, in certain countries (such as Hungary and Italy) during a search at lawyers' premises, the presence of a public prosecutor or a judge is required.[171] Similar provisions exist in Belgium, where an investigating judge and a Bar representative are present during a search.

With reference to search of data outside lawyers' offices, such as data stored in the cloud, often the protection provided is notably weaker than the rules relating to searching of physical premises. In fact, although storage of electronic data is most common in the modern context, government power to access such data is less regulated or limited. For instance, instead of requesting lawyers to provide the electronic data placed outside the office, governments may directly request third parties (as telecommunications service providers or OTT service providers) to provide such information. Therefore, it is noted that, where data is requested from third parties, in some jurisdictions such data may not be expressly covered by professional privilege and, thus, may not receive the same protection as the information located in lawyers' offices.

Government requests to produce information may be formal – that is, with prior obtainment of a court warrant or authorisation – or informal. If the request is informal and where there is no law and no agreement between the lawyer and the service provider expressly preventing such practices, there may be the risk of service providers voluntarily giving government access to the information. Moreover, according to several domestic systems, in case of an urgency, search and seizure may be carried out without a prior court authorisation. However, in such a case an ex post court approval is desirable.

Considering all the above, the protection granted in the physical world should be extended to the electronic world. Therefore, the introduction/amendment of domestic laws may be needed in order to limit possible breaches of professional secrecy and to duly protect the right to a fair trial and defence. In order to balance government interests and the protection of professional privilege, governments seeking to fight terrorism and other serious crimes may be allowed to search and seize data protected by professional secrecy, but only (1) in case of absolute necessity; (2) for the purpose of protecting a concrete and demonstrable public interest; and (3) where there is a concrete concern that the lawyer may be involved in a serious crime. Moreover, government access should be carried out in a targeted manner and subject to prior review by a court or other independent body. In addition, as already highlighted in this paper, the data collected/stored shall be relevant – and not excessive – in relation to the investigation and shall be retained only for a reasonable limited period of time. Finally, specific search and seizure procedures shall be adopted in order to appropriately regulate any access to data held or generated by lawyers, including notification of the Bar the lawyer belongs to, as well as close supervision by a court or other independent body.

171 See Council of Bars and Law Societies of Europe, 'CCBE Comparative Study on Governmental Surveillance of Lawyers' Data in the Cloud', 2014, www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Position_papers/EN_ITL_20140404_Comparative_Study_on_Governmental_Surveillance_of_Lawyer_s_Data_in_the_Cloud_final.pdf accessed 15 August 2018.

APPENDIX A: Proposed principles

1. The principles should define the following terms:
    - 'government'
    - 'access'
    - 'personal data/personal information'
    - 'privacy'
2. Any provisions that provide for government access should be specific and focused, having due regard to the personal data involved and implication of access to this data for fundamental rights.
3. Government access should be allowed only (1) in case of strict necessity, and (2) for the purpose of protecting a concrete and demonstrable public interest.
4. The data collected must be relevant – and not excessive – in relation to the purposes for which they are collected.
5. Retention is a core component that enables access to data. As such, any provisions that mandate retention should be subject to the requirements of legality, necessity and proportionality. Data should only be retained and preserved for a limited period, no longer than the time required for the purpose for which such data is collected.
6. Fundamental rights should be honoured, but these rights are not absolute; thus, balance is needed. These rights can be encroached when there is a justified, overriding government interest. However, that interest should be clearly and concisely defined and any interference with fundamental rights should be subject to strict safeguards and oversight.
7. An independent body (whether that's the judiciary, tribunal or an administrative body) should balance the rights and interests involved.
8. Data is expansive in its scale and scope. Given the revealing nature of data, policies should cover both systematic and targeted access, ensuring fundamental rights are protected under both frameworks. This must include applying more stringent rules on systemic access.
9. Recognising the unique position of electronic communications service providers in granting access to IT systems, these providers should take care to ensure any access request complies with the rule of law and relevant human rights standards. This should apply to not only traditional telecommunications service providers, but those who provide OTT services as well.
10. The current mechanisms to gain cross-border access to data are slow and laborious. In order to ensure effective access can be maintained across jurisdictions, new measures must be created to facilitate trans-border access. These can take the form of (a combination of) multilateral treaties, model laws or self-regulation.

11. Safeguards must be implemented to protect the rights of the persons affected.

12. In gaining access, those authorities involved must be subject to strict accountability and transparency measures. Transparency in the process is paramount.

13. Recognising the importance of privileged and sensitive data, and in particular, legal professional privilege, additional safeguards must be in place before access to this type of information is granted.

14. Given the significance of data for society, businesses and governments, there must be active engagement between relevant parties in determining governance frameworks. Multi-stakeholder collaboration and the development of collaborative strategies between businesses, investors, industry associations, civil society organisations and academics should be promoted to address the unique implications of access to data.

APPENDIX B: Relevant cases

Even if the legislation of a country is rather permissive concerning a government's access to data, that does not imply that the legislation is easy to enforce. Many governments have faced enforcement challenges to enforce its competencies, as will be demonstrated in the cases below.

Cases relating to specific platforms

Yahoo!

On 12 December 2017, the Superior Court of Justice of Brazil ('STJ') ruled on a case[172] involving Yahoo! on the one side and the Federal District of Brazil and the Prosecutor's Office on the other. The case concerned the obligation of the internet provider to disclose data to authorities for the purposes of criminal investigations. Yahoo! refused to disclose the data arguing that the actual internet provider responsible for the keeping of such data was the foreign company Yahoo, Inc. It also alleged that Brazilian authorities needed to follow an international cooperation procedure to obtain the relevant data. STJ decided that the international cooperation procedure was not necessary for Yahoo! to disclose the data, since it has business in Brazil and must abide by the local laws, in accordance with subsection 2, Article 11 of the Marco Civil Law of the Internet in Brazil.

- *Belgium v Yahoo! (Belgian Court of Cassation 1 December 2015, AR P 13.2082 N, RABG 2016, No 7, 485).*

On 1 December 2015,[173] the Belgian Court of Cassation dismissed an appeal lodged by Yahoo! against the ruling of the Court of Appeal of Antwerp of 20 November 2013, which obliged Yahoo! to disclose the identity of the persons who committed fraud using their Yahoo! email addresses. In its decision, the Court of Cassation ruled that there was no issue of extraterritorial jurisdiction at stake. The request for disclosure to an operator of an electronic communications network or an electronic communications service provider who is active in Belgium does not involve any intervention outside the Belgian territory. The Court also found that Yahoo! voluntarily submits itself to Belgian law by using the domain name '.be' or by displaying ads based on its users' location.

Facebook

On 12 September 2017, a similar case involving Facebook in Brazi[174] was ruled by the STJ. Facebook refused to comply with a previous decision of the State Court of Rio de Janeiro that determined, under Article 4 of the Wiretap Act, that it must provide the Federal Prosecutor's Office with information regarding the records of a user to help with a criminal investigation. Facebook alleged that this would not be technically feasible and that the party to the lawsuit should be the foreign company Facebook Miami, Inc. For the same reasons of Yahoo!'s case, the decision was upheld by the STJ.

172 Appeal in thzze Writ of Mandamus No 55.019-DF.

173 *Belgian Court of Cassation 1 December 2015*, AR P 13.2082 N, RABG 2016, no 7, 485 http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=N-20151201-1 [in Dutch] accessed 21 July 2020.

174 Appeal in the Writ of Mandamus No 54.444-RJ.

- *Maximillian Schrems v Data Protection Commissioner [C-362/14 Maximilian Schrems* v *Data Protections Commissioner [2015] ECLI 650].*

In *Schrems* the CJEU annulled on 6 October 2015 the EU/US safe harbour programme for failure to provide an adequate level of protection to personal data transferred from the EU to the US for the following reasons:

  - the mechanism put the needs of US law enforcement officials ahead of the fundamental privacy rights of EU citizens by allowing US law enforcement unfettered access to the transferred data;
  - the Safe Harbour rules offered EU citizens no judicial means of redress in the US;
  - the Safe Harbour decision denied EU Data Protection Authorities the power to review complaints challenging the validity of data transfers to third parties; and
  - US legislation authorised, on a general basis, the storage of all personal data of all the persons whose data is transferred from the EU to the US without any differentiation, limitation or exception being made in light of the objectives pursued, and without providing an objective criterion for determining limits to the access and use of this data by public authorities.

- *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems [C311/18 Data Protection Commissioner* v *Facebook Ireland Ltd, Schrems (9 May 2018, pending)].*

In what is known as *Schrems 2.0*, a reference for preliminary ruling has been submitted to the CJEU. There are a number of issues that have been referred to the Court. The case largely seeks to determine whether standard contractual clauses, that Facebook and other businesses use, provide proper protection for EU citizens' data in line with the obligations set out in EU law and under the Charter of Fundamental Rights. At issue is whether, when personal data is transferred by a private company from an EU Member State, to a private company in a third country for commercial purposes, it may then be further processed in the third country by its authorities for the purposes of national security and law enforcement. If so, does EU law (including the Charter of Fundamental Rights and the ECHR) apply to the transfer or, in determining whether there is a violation of rights or should domestic laws (here, those of the US) be used to assess the protection of individuals' fundamental rights.

WhatsApp

- *Re WhatsApp (Brazil) 2nd Criminal Court of Duque de Caxias (19 July 2019).*

Several cases have been decided in Brazil since 2015 regarding the intention of authorities to force WhatsApp to provide them with useful data for criminal investigations.[175] In these cases, WhatsApp claimed that due to its end-to-end encryption it would not be possible to comply with such requests. Regardless of these arguments, the judges were not convinced and determined the disclosure of data. The rulings stated that if WhatsApp refused to comply therewith, its activities could be suspended. In the most recent case, the STJ has suspended a ruling ordering mobile phone companies to indefinitely block access to WhatsApp. The Rio de Janeiro judge Daniela Barbosa ruled that access to the application should be

175 For instance, Process No 0013872-87.2014.8.18.0140-PI, Process No 201655090143-SE, Process No. 201655000183-SE and Police Investigation No 062-00164/2016-RJ.

blocked immediately because WhatsApp's owner, Facebook, had shown 'total disrespect for Brazilian laws'. But hours later, her ruling was reversed by STJ president at the time, Justice Ricardo Lewandowski, who said that this measure it seemed 'scarcely reasonable or proportional'. In his decision, the Chief Justice stressed how people from across Brazil rely on WhatsApp to communicate with others every day, and that they bear the greatest burden when the service is blocked.

Microsoft

- *United States* v *Microsoft Corp., 584 US (2018).*

- In July 2016, the Second Circuit ruled that Microsoft did not have to turn over data (in this case, emails) stored in its Irish data centre in response to an SCA warrant. The warrant had been issued on showing of probable cause that the account was being used in furtherance of a drug trafficking case. The Court found that the SCA could not be applied extraterritorially, and thus could only be relied on to authorise warrants to seize data stored in the US. On 16 October 16, 2017, the SCOTUS granted review of this ruling. In December 2017, the EC submitted an amicus curiae to the SCOTUS which discusses the issue of jurisdiction and the application of the GDPR.

On 18 April 2018, the SCOTUS ruled that there was no ongoing live dispute to decide in the *Microsoft* case. This was a direct result of the enactment of the CLOUD Act. The CLOUD Act amends the SCA by adding the following:

> 'A service provider shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States'.[176]

Instagram[177]

On 14 February 2018, Roskomnadzor ordered Instagram to take down a video alleging that Deputy Prime Minister Sergei Prikhodko took a bribe from oligarch Oleg Deripaska. The video was designed by the Russian opposition leader, Alexey Navalny. The social media company had three days to comply with the order, which it did. Otherwise, Roskomnadzor would have blocked the whole website.

Skype

- *Skype Communications SARL [Correctional Court of Mechelen 27 October 2016, ME20.F1.105151-12.].*

On 15 November 2017, the Court of Appeal of Antwerp confirmed a judgment of the Correctional Court of Mechelen of 27 October 2016 condemning Skype Communications SARL, based in Luxembourg, for refusing to install a wiretap equipment (as ordered by an investigating magistrate in Mechelen). The wiretap was ordered to register communications of a Skype user. On jurisdiction, the Court applied a reasoning analogous to the *Yahoo!* case (see above), by holding that the refusal to cooperate on the part of

176 CLOUD Act, as part of the Consolidated Appropriations Act 2018 Pub L 115-141 ss 103(a)(1).

177 'Instagram submits to Russia censor's demands' BBC News (15 February 2018) www.bbc.co.uk/news/technology-43070555 accessed 4 September 2018.

the 'telecom' operator can be deemed to have occurred in the place where the information should have been received, regardless of where the operator was established.

Telegram[178]

- *Roskomnadzor* v *Telegram No 2-1779/2018.*

On 14 September 2016, Russian FSB demanded that Telegram, a Russian-based messenger, surrender its universal encryption key on all user correspondence to the FSB. After the company refused to comply, it was fined RUB800,000 following the decision of a Russian court. Telegram insists that it is impossible from a technical perspective to turn over the encryption keys as they are generated on users' own devices. As a result, Telegram's administrators have no overview of encryption keys themselves. Moreover, in December 2017 the company decided to appeal the court's decision within the UN.[179] A letter was prepared for the attention of David Kaye, the UN's Special Rapporteur on promoting and protecting the right to freedom of opinion and expression, where Telegram had a chance to flag their concerns.

LinkedIn

- *Roskomnadzor* v *LinkedIn Corporation No 33-38783/2016.*

On 17 November 2016, *Roskomnadzor*, which decision was supported by local Moscow courts,[180] included LinkedIn on the Register of Personal Data Infringers and ordered telecommunication providers to block access to the social media platform in the territory of Russia. The reason for such decision was LinkedIn's failure to adhere to the data localisation requirement (failure to physically keep storage sites with the personal data of Russian users on the territory of Russia) as well as collection of personal data without obtaining an appropriate level of data subjects' consent. For the purposes of deliberations, the courts inspected publicly available information and the social media platform itself – no other detailed investigations have been launched.

Cases relating to privacy and fundamental rights

- *Digital Rights Ireland v Minister for Communications & Ors and Michael Seitlinger & Ors (Joined Cases C-293/12 and C-549/12) [2014] 2 All ER.*

On 8 April 2014, the Grand Chamber of the CJEU delivered a judgment concerning the legality of Directive No 2006/24/EC (commonly referred to as the 'Data Retention Directive'), which required the providers of publicly available electronic communications services or public communications networks to retain traffic and location data belonging to individuals or legal entities.

The Directive was challenged by the High Court of Ireland and the Constitutional Court of Austria, in adjudicating cases, on the grounds of infringement of the right to private life and the right to

178 Scan of the FSB request: https://vk.com/doc1_451499493?hash=f45613990541c82af8&dl=136a40c575bfa82136.

179 Damir Gainutdinov, 'Letter to David Kaye, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' (14 December 2017) https://ccla.org/cclanewsite/wp-content/uploads/2017/12/AGORA_Submission-EN.pdf accessed 18 August 2018.

180 Extract from the court's decision [in Russian]: http://mos-gorsud.ru/mgs/services/cases/appeal-civil/details/19d661b0-6b14-48eb-b753-9adbf19fe32a accessed 21/7/2020.

the protection of personal data of individuals (protected under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union).

In this decision, the Court affirmed that the retention of such data – including text message senders and recipients and call histories – allows for 'very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained' and that the national legislation adapted in relation to the Directive exceeded 'the limits of what is strictly necessary and cannot be considered to be justified within a democratic society'. Moreover, the Court held that the retention of data to allow access by the competent national authorities constitutes processing of data and, therefore, affects the right to private life and the protection of personal data.

The CJEU held that Directive 2006/24/EC did not contain sufficient safeguards to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. The CJEU also affirmed that EU Member States seeking to fight a 'serious crime' are allowed to retain data in a targeted manner but must be subject to prior review by a court or independent body. Based on the foregoing, the CJEU held the Directive invalid.

- *Big Brother Watch & Ors v United Kingdom App No 58170/13, 62322/14, and 24960/15 (ECtHR 13 Sept 2018).*

On 13 September 2018, the ECtHR ruled on the surveillance regime for obtaining communications data found under the Regulation of Investigatory Powers Act 2000 (RIPA).[181] The case was concerned with the issue of bulk interception provided for in that Act. The applicants alleged that the bulk interception regime violated Article 8 of the ECHR as there was insufficient oversight in the selection of relevant criteria for interception and filtering the communications for examination. The Court held that there was an interference with Article 8. In particular, the lack of safeguards meant that the domestic statute did not meet the 'quality of law' requirement of the Convention and the interference was therefore not 'necessary in a democratic society'. The overall impact of the *Big Brother Watch* case is mixed. While the court did find that the regimes at issue were an interference, they also held that mass surveillance was not categorically disproportionate. Nor did they find that prior judicial authorisation was an absolute necessity, recognising it to be best practice but not in itself sufficient to ensure compliance. However, the case did hold that the distinction between content and metadata was not viable in adjudging privacy violations.

- *Riley* v *California 573 US (2014).*

Riley was stopped for a traffic violation, which subsequently led to his arrest for weapons charges. During the course of his arrest, a cell phone was seized from Riley's pocket and the information was accessed. Based on the information found in the search, further charges were filed against Riley. Riley argued that the cell phone evidence should have been suppressed based on the failure of the police to obtain a warrant prior to the search of the phone. The SCOTUS held that police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.

- *Carpenter v United States No 16-402, 585 US (2018).*

181 *Big Brother Watch & Ors v United Kingdom* App no 58170/13 (ECHR 13 Sept 2018).

The case of *Carpenter* concerned the use of cell-site location information (CSLI) in the investigation of crime. This information provides precise and clear records of the location and movements of cell phones. In Carpenter's case, the government was able to obtain the records of Carpenter's movements over the course of 127 days for the purposes of forming a case against him. These records were obtained without a warrant supported by probable cause. Carpenter argued that such actions were a violation of the Fourth Amendment. The court, in holding that the actions did represent a search under the Fourth Amendment, noted the unique nature of cell-site records and the information they could reveal. In finding that there was a privacy interest in the information obtained, the Supreme Court held that it was necessary for the government to obtain a warrant based on probable cause in order to access this type of information.

Finally, it should be noted that while some jurisdictions have vast case law on the matter, this is not the case for every country. Accordingly, there have been no reported cases in Australia of agencies attempting to access information held by ISPs or other data aggregators or of data subjects seeking protection against government entities in relation to their attempts to h collect information about them. This perhaps suggests both the breadth of statutory powers available to agencies to compel access and the cooperative attitude of the communications and technology companies.

To view online, visit: **https://www.ibanet.org/LPRU/Cybersecurity.aspx**

To find out more, email: **LPRU@int-bar.org**