NEW GLOBAL DEVELOPMENTS IN DATA PROTECTION AND PRIVACY REGULATIONS: COMPARATIVE ANALYSIS OF EUROPEAN UNION, UNITED STATES, AND RUSSIAN LEGISLATION

ANNE WRIGHT FIERO* & ELENA BEIER**

* Anne Wright Fiero is a Senior Corporate Counsel at Amazon Web Services, Inc. She thanks her colleague and co-author, Elena Beier, for her insightful comments and collaboration.

** Elena Beier is a managing partner at Beier & Partners. She would like to express her gratitude to Anne Fiero for her co-authorship and expertise.

I. INTRODUCTION

Privacy is a fundamental human right recognized in constitutions, international treaties, and national legislation around the globe. The era of globalization and rapid technology development highlights multiple risks to privacy rights. Such developments make it more important than ever to enact legal frameworks for data protection on a national and global scale. Fully applicable across the European Union (EU) as of May 2018, the General Data Protection Regulation (GDPR) is the most comprehensive and progressive piece of data protection legislation in the world.[1]

The intent of this Article is to provide an overview of EU, U.S., and Russian data privacy regulations, as influenced by the GDPR and the countries' respective cultural and business traditions of privacy.[2] More specifically, we explore how the historical, cultural, legal, business, and political traditions in each country have shaped the laws and regulations in their respective jurisdictions. As described in Part III, the U.S. approach tends to be *ad hoc* and focused on concepts like personal freedom and non-interference by the state. Explored in Parts II and IV, the more uniform European approach tends to focus on the dignity of individuals and their protection—not only against the state but also against private companies and other individuals. In the last few years, U.S. society has focused more closely on data privacy concepts, with recent scrutiny on credit history checks, social media networks, and sharing other attributes of everyday American life, concepts that have long been considered invasive for many Europeans. The European privacy mentality has also been largely influenced by its historical and political systems, such as European monarchies, the Nazi regime in Germany, and the totalitarian regime in the Soviet Union, under all of which disclosure of personal information could lead to severe consequences and prosecutions. Thus, protection of private information is ingrained in European society.

In Part V, we touch on specific areas of privacy regulations, such as the cross-border transmission of data which presents multiple unique privacy-related

---

[1] Commission Regulation of 27 April 2016, 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, 2016 O.J. (L 119) 48 [hereinafter General Data Protection Regulation].

[2] This article is current as of January 2022. Subsequent changes in data protection and privacy regulation are not addressed.

challenges. Finally, we conclude by inviting the adoption of a more consistent, globalized regulatory approach to data protection.

II. EU REGULATIONS

For several decades, the EU has been a pioneer in privacy and data protection. The right to data protection and the right to privacy are two distinct human rights recognized in the Charter of Fundamental Rights of the European Union, the Treaty on the Functioning of the EU (TFEU), and other EU regulations. Article 8 of the Charter of Fundamental Rights of the European Union declares:

> [E]veryone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.[3]

TFEU, Article 16 declares:

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.[4]

Likewise, the EU Data Protection Directive of 1995 (Directive 95/46/EC) was the first European document to declare the necessity of balancing the free circulation of information in EU countries and guarantees of human rights protection, including the protection of personal data.[5] This Directive (which required implementation in national legislation) satisfied the needs of the economy and technology in 1995.[6] However, the rapid technological changes of recent years has demanded a heightened level of protection.

---

[3] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012 OJ L. C 236/391, Art. 8, https://perma.cc/M3AG-PT9T.

[4] Consolidated Version of the Treaty on the Functioning of the European Union 2012 O.J. (C 326) 47 [hereinafter TFEU].

[5] European Union, Data Protection Directive, 24 October 1995, 95/46/EC, https://perma.cc/UKY4-TPVH.

[6] *Id.*

On May 25, 2018, the European Parliament's regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, known as the GDPR, became effective, changing the former legislation of the European Union on personal data.[7] On account of the global nature of business, including the Internet-based and cloud-computing businesses, the effects of the GDPR have been felt far beyond the borders of the EU.

A. Overview of the GDPR

The GDPR, unlike former Directive 95/46/EC, was directly effective in all member states.[8] "Direct effect" is the core principle of application of the EU law.[9] According to this principle, private individuals in addition to legal entities can protect their rights by referring to community standards in national courts.[10] The main objective of the GDPR is privacy protection in the processing of data, free moving of personal data,[11] and the unification of European law surrounding the processing of personal data.[12] The GDPR applies to organizations engaged in "professional or commercial activity."[13]

Article 4(1) of the GDPR defines personal data as:

> [A]ny information relating to an identified or identifiable natural person ('data subject'); identifiable individual is a person who can be identified directly or indirectly, in particular, by reference to such an identifier as a name, identification number, location data, network identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[14]

Article 4(2) introduces the concept of processing, which can be "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not they are performed by automatic means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[15] The controller in accordance with Article 4(7) is an individual or legal entity, state body, agency, or other body that independently or together with others determines the goals and means of processing personal data; if the goals and means of such

---

[7] *See* General Data Protection Regulation, *supra* note 1.

[8] TFEU art. 288.

[9] *See, e.g.*, European Parliament, *Parliamentary Questions P-003121/2018*, 13 July 2018, https://perma.cc/YNM4-JQ6U.

[10] *See, e.g.*, Case 26/62, N.V. Algemene Transp. en Expeditie Onderneming van Gend & Loos v. Neth. Inland Revenue Admin., 1963 E.C.R. 1, 7.

[11] General Data Protection Regulation, *supra* note 1, art. 1.

[12] *Id.* Recital (3).

[13] *Id.* art. 4.

[14] *Id.* art. 4.

[15] *Id.* art. 4(2).

processing are determined by the legislation of the Union or a member state, the controller or specific criteria for its appointment may be provided for by the legislation of the Union or a member state.[16] The processor in accordance with Article 4(8) is an individual or legal entity, a state body, agency, or other body that processes personal data on behalf of the controller.[17]

Apart from these new definitions, the GDPR introduces new principles of processing personal data such as fairness;[18] lawfulness of processing;[19] transparency;[20] collection for specified, explicit and legitimate purposes;[21] data minimization: adequate, relevant, and limited to what is necessary;[22] accuracy of data: where necessary and kept up to date;[23] and processing in a manner that ensures appropriate security of the personal data.[24]

B. Other Novel Concepts Introduced in the GDPR

Significant novel concepts introduced in the GDPR include extraterritorial jurisdiction,[25] the right to be forgotten,[26] and stricter rules for obtaining consent.[27]

According to the GDPR, the territorial application of the law applies to:

> [T]he processing of personal data in the context of the activities of the institution of the controller or processor in the Union, regardless of whether processing occurs in the Union or not. This Regulation applies to the processing of personal data of data subjects located in the Union, by a controller or processor not established in the Union, where the processing activities are related to: the offer of goods or services, regardless of whether the payment of the data subject is required to such data subjects in the Union; or control over their behavior to the extent that this happens in the Union. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the laws of the Member States are applied on the basis of public international law.[28]

Based on the above, the GDPR affects not only companies present within the territory of the EU, but also non-residents selling goods or services in the EU or companies monitoring the data of EU citizens. Recital 23 of the GDPR mentions such factors as the "use of a language or a currency generally used in one or more Member States

---

[16] *Id.* art. 4(7).
[17] *Id.* art. 4(8).
[18] *Id.* art. 5.1(a).
[19] *Id.*
[20] *Id.*
[21] *Id.* art. 5(b).
[22] *Id.* art. 5.1(c).
[23] *Id.* art. 5.1(d).
[24] *Id.* art. 5.1(f).
[25] *Id.* art. 3.
[26] *Id.* art. 17.
[27] *Id.* arts. 4(11), 7; Recitals 32, 42.
[28] *Id.*

with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union."[29] These factors may make it apparent that the company "envisages offering goods or services to data subjects in the Union."[30] Moreover, services to data subjects are "irrespective of whether connected to a payment."[31] These changes affect a wide range of companies in different sectors of the economy such as financial services, technology, media, education, logistics, pharma and clinical research, e-commerce, and many others.

The data subject has the right to obtain the erasure of his personal data without delay.[32] In this case the controller is obliged to erase personal data without delay, provided that such personal data is no longer necessary in relation to the purposes for which it was collected, the data subject withdraws consent on which the processing is based, the personal data has been unlawfully processed, or in some other use cases.[33] It is therefore essential that all informational systems of the company must be set in such a way that any data can be removed forever.

The data subject's consent must be concrete, informed, and expressed freely, and it is subject to withdrawal at any time.[34] Requests for such consent need to be clear, in simple language, and distinguishable from the other matters requiring consent.[35] The GDPR has additional conditions applicable to data of a child:

> [T]he processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child . . . the controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.[36]

To enforce its provisions, the GDPR sets multilevel sanctions for infringements of personal data and allows law enforcement agencies to apply fines capable of presenting significant financial risks for companies: up to 4% of annual revenue or €20 million in cases of non-compliance with an order from the supervisory authority.[37] Other infringements, related to the obligations of the controller and the processor, certification and monitoring body, and some others, could result in a fine up to 2% of annual revenue or €10 million.[38]

Illustration of these GDPR regulations makes it clear that European legislation emphasizes the importance of protecting the rights of data subjects while at the

---

[29] *Id.* Recital 23.
[30] *Id.*
[31] *Id.*
[32] *Id.* art. 17.
[33] *Id.*
[34] *Id.* arts. 4, 7.
[35] *Id.* art. 7.
[36] *Id.*
[37] *Id.* art. 83.5.
[38] *Id.* art. 83.4.

same time setting complicated but solvable tasks for companies who require legal and technical assistance in order to comply with the GDPR.

C. GDPR Fines and Their Significance for Global Business

In the three years since the GDPR came fully into effect, case law is continuing to evolve. According to the European Data Protection Board's (EDPB) February 2019 report on the implementation of the GDPR, 206,326 cases were reported by supervisory authorities in thirty-one EU countries in the first nine months of the GDPR's application.[39] Of these, 94,622 related to complaints and 64,684 to data breach notifications by data controllers.[40] The Netherlands, Germany, and the UK had the most data breaches notified to supervisory authorities.[41]

According to EDPS's 2020 Annual Report, the number of complaints in 2020 increased 23% compared to 2019.[42] The EDPS's 2021 Annual Report shows the number of complaints in 2021 increased by 33% compared to 2020.[43] As of September 2021, GDPR fines issued by European Data Protection Authorities total just over €1.3 billion, with nearly half of GDPR fines levied against tech companies and telecommunications operators.[44]

The French Data Regulator, Commission Nationale de l'Informatique et des Libertés (CNIL), issued one of the earliest and largest GDPR fines (€50 million) against Google.[45] In its 2019 decision, the CNIL found that Google breached the GDPR by (1) failing to provide a transparent explanation of how and why it used personal data and (2) failing to obtain sufficient consent for ad personalization, as it was not "sufficiently informed," "specific," or "unambiguous."[46] The CNIL concluded that consent based on consumers clicking a blanket opt-in clause does not go far enough because the GDPR requires consent to be given distinctly for each purpose.[47]

Other notable GDPR fines in 2020 and 2021 include:

---

[39] EUROPEAN DATA PROTECTION BOARD, FIRST OVERVIEW ON THE IMPLEMENTATION OF THE GDPR AND THE ROLES AND MEANS OF THE NATIONAL SUPERVISORY AUTHORITIES (2019), https://perma.cc/R2M7-SQKS. Data Protection authorities are independent public entities that supervise—through investigative and corrective powers—the application of the GDPR. A list of national Data Protection Authorities can be found here: *Our Members*, EUR. DATA PROT. BD., https://perma.cc/A3E2-JPNM.

[40] FIRST OVERVIEW ON THE IMPLEMENTATION OF THE GDPR, *supra* note 39.

[41] *Over 59,000 Personal Data Breaches Reported Across Europe Since Introduction of GDPR, According to DLA Piper Survey*, DLA PIPER (Feb. 6, 2019), https://perma.cc/9DEQ-WHZE.

[42] EUR. DATA PROT. SUPERVISOR, ANNUAL REPORT 2020 38 (2021), https://perma.cc/D7SG-HPTC.

[43] EUR. DATA PROT. SUPERVISOR, ANNUAL REPORT 2021 59 (2022), https://perma.cc/34VT-MG3L.

[44] Justinas Baltrusaitis, *GDPR fines in Q3 almost hit €1 billion, 20x more than in Q1 and Q2 combined*, FINBOLD (Oct. 7, 2021), https://perma.cc/W6YZ-UCZHv.

[45] *See* Jill Goldsmith, *France Slaps Google With €50M Fine For Privacy Violation Under GDPR*, FORBES (Jan. 21, 2019), https://perma.cc/9KB7-YAHP.

[46] *Id.* ("Google does not spell out why it is using personal data, how long the data stored [sic], or what categories of data uses [sic] for ad-targeting . . . Key information is 'excessively disseminated across several documents, with buttons and links on which it is required to click . . . implying sometimes up to 5 or 6 actions.'").

[47] *Why France hit Google with a whopping €50 million fine*, THE LOCAL (Jan. 21, 2019), https://perma.cc/NCW2-7AEZ.

Year	Size of Fine	Fined Entity	Supervisory Authority	Reason for fine
2020[48]	€35 million	H&M (clothing retailer)	Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI)	Breach involved improper processing of sensitive data related to employee's vacation and sick leave.
2020[49]	€28 million	Telecom Italia	Italian DPA (Garante)	Series of alleged infractions and violations stemming from an overly aggressive marketing strategy. Millions of individuals were bombarded with promotional calls and unsolicited communications, some of whom were on non-contact and exclusion lists.
2020[50]	€220 million	British Airways	UK DPA (ICO)	2018 data breach that impacted 500,000 customers. Hackers accessed log-in details, payment card information, and travelers' names and addresses.
2020[51]	€20 million	Marriott	ICO	Significantly below the $123 million fine the ICO originally said they would levy based on allegations that hotel chain's guest reservation database was compromised. Personal data like guest names, addresses, passport numbers, and payment card information was exposed.
2020[52]	€17 million	Wind	Italian DPA	Direct marketing activities that included spamming Italians with ads without their consent and providing incorrect company contact information, leaving consumers unable to unsubscribe.

[48] *Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre*, EUR. DATA PROT. BD. (Oct. 2, 2020), https://perma.cc/LQ3B-LU7R.

[49] *Marketing: The Italian SA Fines TIM EUR 27.8 Million*, EUR. DATA PROT. BD. (Feb. 1, 2020), https://perma.cc/3DK6-TG8B.

[50] *ICO Statement: Intention to Fine British Airways £183.39m Under GDPR for Data Breach*, EUR. DATA PROT. BD. (July 8, 2019), https://perma.cc/4D2N-GAT7.

[51] *ICO Statement: Intention to Fine Marriott International, Inc. More Than £99 Million Under GDPR for Data Breach*, EUR. DATA PROT. BD. (July 9, 2019), https://perma.cc/4ERT-N6FC.

[52] *Telephone Operators: Italian SA Fines Wind EUR 17 Million and Iliad EUR 0.8 Million*, EUR. DATA PROT. BD. (July 27, 2020), https://perma.cc/68PA-BC56.

2020[53]	€12 million	Vodafone Italia	Italian DPA	Several alleged data processing issues including failing to properly secure customer data and sharing personal data with third-party call centers.
2021[54]	€746 million	Amazon Europe Core S.à.r.l	Luxembourg's National Commission for Data (CNDP)	GDPR breaches related to the gathering of cookie consent.
2021[55]	€225 million	WhatsApp Ireland Ltd.	Irish DPA (DPC)	GDPR breaches in relation to the provision and transparency of information to users and non-users of WhatsApp.
2021[56]	€10 million	Notesbooks-billiger.de (NBB) (German electronics retailer)	Lower Saxony DPA	NBB's alleged use of CCTV cameras to monitor its employees and customers.

Introducing such novel concepts into data privacy regulations significantly changed the EU and global data privacy law frameworks. Stricter rules, detailed regulations for processors and controllers, extended rights for natural persons, as well as the significant fines imposed on companies, demonstrate the emerging data privacy trend within the EU, which is to acknowledge privacy as an important human right in today's world and to strive for a proper balance between privacy rights and other human rights. The extraterritorial jurisdiction of the GDPR allows it to extend its regulations to non-EU countries if companies located therein wish to do business with EU customers.[57] This novel approach is problematic for non-EU companies targeting the personal data of European Union residents: Such companies likely face the challenge of complying with both their domestic and EU regulations. The extraterritorial application of the GDPR could also be characterized as a change to the existing direct effect doctrine of EU law, which originally implied that only member states of the European Union are bound to some acts of its legislation without any further implementation.[58]

---

[53] *Aggressive Telemarketing Practices: Vodafone Fined Over 12 Million Euro by Italian DPA*, EUR. DATA PROT. BD. (Nov. 19, 2020), https://perma.cc/G8HT-XS9Y.

[54] *Luxembourg DPA Issues €746 Million GDPR Fine to Amazon*, DATA PRIVACY MANAGER BLOG (July 20, 2021), https://perma.cc/3P2L-NSJD.

[55] *Data Protection Commission Announces Decision in WhatsApp Inquiry*, DATA PROT. COMM'N. (Sept. 2, 2021), https://perma.cc/PN2B-3T6A.

[56] *State Commissioner for Data Protection in Lower Saxony Imposes €10.4 Million Fine Against notebooksbilliger.de*, EUR. DATA PROT. BD. (Jan. 26, 2021), https://perma.cc/5YPY-AY34.

[57] General Data Protection Regulation, *supra* note 1, art. 3.

[58] *See, e.g.*, Case 26/62, N.V. Algemene Transp. en Expeditie Onderneming van Gend & Loos v. Neth. Inland Revenue Admin., 1963 E.C.R. 1, 13.

D. Other EU Industry Specific Data Privacy Regulations

Like the U.S. and Russian frameworks that will be detailed below, the EU has adopted data privacy regulations that are industry specific.

1. Healthcare

The EU's role in the field of public health, as established by the Treaty on the Functioning of the EU, is limited to complimenting the national policies of EU Members, coordinating their actions, and facilitating the communication and exchange of data between the European Commission and its members.

Decision No 1082/2013/EU of the European Parliament and the Council (22 October 2013) concerned serious cross-border threats to health and repealed Decision No 2119/98/EC. It established a framework for public health regulation at the EU level.[59] The Decision laid down rules on epidemiological surveillance,[60] monitoring, early warning, and combating serious cross-border threats to health, including preparedness and response planning related to those activities, in an effort to coordinate and complement national policies.[61] Article 16 specifically addresses personal data protection in cross-border health threats, stating that personal data shall be processed in accordance with Directive 95/46/EC (now the GDPR) and European Council Regulation No 45/2001. Moreover, it provides that appropriate technical and organizational measures shall be taken to protect such personal data against accidental or illegal destruction, accidental loss, or unauthorized access and against any form of illegal processing.[62]

The Early Warning and Response System (EWRS) also established by the Decision includes a selective messaging functionality that allows personal data to be communicated only to national competent authorities involved in contact tracing measures.[63] The selective messaging functionality is designed and operated to ensure the safe and lawful exchange of personal data.[64]

When competent authorities implementing contact tracing measures communicate the necessary personal data through the EWRS, they must use the selective messaging functionality and can only communicate the data to the other Member States involved in the contact tracing measures.[65] Messages containing personal data are automatically erased twelve months after the date of their initial posting.[66]

Where a competent authority establishes that the notification of personal data it made is in breach of Directive 95/46/EC (now GDPR) because the notification was unnecessary for the implementation of the contact tracing measures, it is required

---

[59] Council Decision 1082/2013, 2013 O.J. (L 293) 2 (EC).

[60] *Id.* art. 3 ("epidemiological surveillance" means the systematic collection, recording, analysis, interpretation and dissemination of data and analysis on communicable diseases and related special health issues).

[61] *Id.* art. 1.

[62] *Id.* art. 16.

[63] *Id.* arts. 8–9, 16.

[64] *Id.* art. 16.

[65] *Id.*

[66] *Id.*

to immediately inform the Member States to which the breaching notification was transmitted.[67] In relation to their responsibilities to notify and rectify personal data issues through the EWRS, the national competent authorities are regarded as controllers, as is the Commission in relation to its responsibilities concerning the storage of personal data.[68]

On March 16, 2020, the Chair of the European Data Protection Board (EDPB) issued a statement on the processing of personal data in the light of the COVID-19 pandemic.[69] The statement specifies that EU data protection law does not restrict state actions necessary to fight the pandemic.[70] More specifically, GDPR allows the processing of personal genetic, biometric, and health concerning data if it is necessary "for reasons of public interest in the area of public health,"[71] "to protect the vital interests of the data subject or of another natural person,"[72] or "for compliance with a legal obligation."[73] These provisions indicate that the EDPB is open to the possibility of allowing companies to engage in the collection of personal data of their employees and others, including their personal health data, to prevent the spread of the disease, so long as it is done proportionately.

Multiple governments around the globe decided to disregard fundamental privacy regulations in the name of tackling the pandemic. For example, the Hungarian Government, on May 4, 2020, issued a Decree containing several provisions extensively affecting data protection in Hungary for the duration of the state of emergency caused by COVID-19.[74] It stipulated that the one-month time limit for Controllers to provide the necessary information, as required by Article 12 of the GDPR, starts only after the termination of the state of emergency for any COVID-19-related data subject requests.[75] Moreover, the data collection information requirements for Controllers, as provided in Articles 13 and 14 of the GDPR, will be satisfied by publishing an electronic privacy notice giving the purpose and legal basis of the data processing of which data subjects may take notice.[76]

2. *Artificial Intelligence*

The rapid and global development of artificial intelligence raises serious legal concerns. While artificial intelligence (AI) can optimize many processes traditionally operated by humans, it can also jeopardize fundamental human rights. This harm relates to a wide variety of risks: safety and health of individuals, damage to property, loss of privacy, limitations to the right of freedom of expression, and human

---

[67] *Id.*

[68] *Id.*

[69] Press Release, *Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak*, EUR. DATA PROT. BD. (Mar. 16, 2020), https://perma.cc/CB3B-ZVMW.

[70] *Id.*

[71] General Data Protection Regulation, *supra* note 1, art. 9(2)(i).

[72] *Id.* arts. 6(1)(d), 9(2)(I).

[73] *Id.* arts. 6(1)(c), 9(2)(b).

[74] 179/2020. (V. 4.) Korm. r. a veszélyhelyzet idején az egyes adatvédelmi és adatigénylési rendelkezésektől való eltérésről (Governmental Decree No. 179/2020 (V.4.) on Derogations from Certain Data Protection and Data Protection Provisions in the Event of an Emergency).

[75] *Id.*

[76] *Id.*

dignity. Therefore, a regulatory framework is necessary to minimize these various risks and potential harms. The main risk related to the use of AI, however, concerns personal data and privacy protection.

In its Communication on AI for Europe, the European Commission provided its first definition of AI:

> [S]ystems that display intelligent behavior by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g., voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g., advanced robots, autonomous cars, drones or Internet of Things applications).[77]

This definition was further refined by the High-Level Expert Group on Artificial Intelligence.[78] On February 19, 2020, the European Commission presented a proposal for comprehensive regulation of artificial intelligence at the European Union level: "White Paper on Artificial Intelligence – A European approach to excellence and trust."[79]

Though the GDPR does not explicitly refer to AI, it broadly regulates the processing of personal data regardless of the technology being used.[80] Thus, any technology that is designed to process personal data, including AI, will fall under its scope. As the European Data Protection Board (EDPB) recently commented, "the GDPR is built in a technologically neutral manner in order to be able to face any technological change or revolution."[81]

When processing personal data using AI systems, controllers should comply with Article 6(1) of the GDPR and its requirements of consent, legitimate interests, legal obligation, or contractual necessity. An appropriate legal basis should be established during both the training and use phases of the AI system.

III. UNITED STATES REGULATIONS

The key regulations governing data privacy in the United States are the U.S. Constitution, federal and state laws and regulations, and international treaties.

---

[77] *Commission Communication on Artificial Intelligence for Europe*, at 1, COM (2018) 237 final (Apr. 25, 2018).

[78] *High-Level Expert Group on Artificial Intelligence on A Definition of AI: Main Capabilities and Scientific Disciplines*, at 7 (Dec. 1, 2018), https://perma.cc/95PT-NNBG ("Artificial intelligence (AI) refers to systems designed by humans that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data and deciding the best action(s) to take (according to pre-defined parameters) to achieve the given goal. AI systems can also be designed to learn to adapt their behaviour by analysing how the environment is affected by their previous actions.").

[79] *Commission White Paper on Artificial Intelligence – A European approach to excellence and trust,* COM (2020) 65 final (Feb. 19, 2020), https://perma.cc/22W9-CFRH.

[80] *Id.*; *see also* CENTRE FOR INFO. POL'Y LEADERSHIP, ARTIFICIAL INTELLIGENCE AND DATA PROTECTION: HOW THE GDPR REGULATES AI 3 (2020), https://perma.cc/A4DM-BAXU.

[81] Response to Member of the European Parliament Sophie in 't Veld's letter on unfair algorithms, European Data Protection Board (Jan. 29, 2020), https://perma.cc/HR6C-MKMM.

A. U.S. Constitution

The U.S. *ad hoc* approach to privacy laws is tethered, at least in part, to the Constitution. While the Constitution explicitly guarantees many rights, it does not have an explicit right to privacy. The Supreme Court has found a right to privacy implied by the terms of other portions of the Constitution,[82] but on a federal level there is no express guarantee to privacy. By contrast, the right to privacy has been explicitly incorporated into many state constitutions.[83]

B. Federal Laws

1. Overview

The United States has not yet developed a single, federal data protection law. Instead, U.S. federal law follows a sectoral approach to data protection legislation that relies on legislation and regulation aimed at specific sectors or industries.[84] Given the lack of comprehensive federal legislation in the United States, the private sector has been given fairly broad latitude to implement its own policies, develop its own technology, and take steps to prevent the dissemination of private data. U.S. federal legislation tends to be sparse and only adopted on an *ad hoc* basis or in a reactionary rather than proactive manner.[85] As described below, state statutes also govern data privacy, and these laws tend to be more focused on protecting individual or consumer privacy rights.

With the passage of California's Consumer Privacy Act (CCPA)—which has since been amended by the California Privacy Rights Act of 2020 (CPRA)—and similarly comprehensive privacy legislation going into effect in Colorado and Virginia in 2023,[86] the push for comprehensive federal privacy law in the U.S. is stronger than ever. Technology companies, including Google, Apple, Intel, and Facebook, have advocated for federal privacy laws, at least in part, to ease the burden of having

---

[82] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485 (1965) ("We have had many controversies over these penumbral rights of 'privacy and repose.' . . . These cases bear witness that the right to privacy which presses for recognition here is a legitimate one.").

[83] *See, e.g.*, ALASKA CONST. art. I, § 22 (the right of the people to privacy is recognized and shall not be infringed); *Ravin v. State*, 537 P.2d 494, 514–15 (Alaska 1975) ("Since the citizens of Alaska, with their strong emphasis on individual liberty, enacted an amendment to the Alaska Constitution expressly providing for a right to privacy not found in the United States Constitution, it can only be concluded that that right is broader in scope than that of the Federal Constitution."); CAL. CONST. art. 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are . . . and privacy."); *San Francisco Apartment Ass'n v. City & Cnty. of San Francisco*, 142 F.Supp. 3d 910, 933 (N.D. Cal. 2015) ("California's constitutional right to privacy is wider than its federal counterpart in that it protects individuals not only against violations by state and federal government entities, but also against violations by other individuals and private companies."); MONT. CONST. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.").

[84] *See* Stephen P. Mulligan & Chris D. Linebaugh, CONG. RSCH. SERV., DATA PROTECTION: AN OVERVIEW 7 (2019).

[85] *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. § 1681; Cable Television Consumer Protection and Competition Act of 1992, Pub. L. No. 102–385, 106 Stat. 1460.

[86] *See infra* Part III.C.

to comply with multiple differing state laws. Google advocates legislation aimed at transparency, portability, broad application, and preemption.[87] Apple advocates for legislation aimed at minimizing the types and amount of data collected from individuals and establishing data encryption that will help consumers to protect and track their data.[88] Intel, a Silicon Valley-based chipmaker, submitted a draft privacy bill to Congress titled "Innovative and Ethical Data Use Act of 2018," most recently updated in May of 2019.[89] Intel's draft bill focuses on technologically neutral provisions that promote the free flow of data, while encouraging funding and research for data security.[90] In February 2019, the U.S. Chamber of Commerce followed suit, submitting a draft bill focused on a consumer's "opt out" privileges and enhanced powers for the Federal Trade Commission (FTC).[91] The Chamber of Commerce model shares many of the tenets of other proposals, with an emphasis on an international scope and a flexible approach to regulation and penalty depending on the types of data at issue.[92] In a March 2019 *Washington Post* op-ed, Facebook CEO Mark Zuckerberg called for GDPR-like legislation in the U.S. and suggested that data privacy required a "more active role for governments and regulators."[93]

Although the U.S. Congress has yet to pass, or even vote on, a federal privacy bill, multiple are pending in the current Congressional term.[94] The 116th Congress held several rounds of hearings concerning federal privacy legislation, including "Policy Principles for a Federal Data Privacy Framework in the United States,"[95] and "GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation."[96] The current Congress held a hearing on "Protecting Consumer Privacy,"[97] but there remains little bipartisan agreement on how to regulate the use, collection, and disclosure of personal information. Regulatory approaches to data privacy tend to focus on whether the aggregation of data amounts to unfair or anticompetitive behavior.[98] Cameron Kerry, a former General Counsel and Acting Secretary of the U.S. Department of Commerce, notes, "[w]ithout baseline privacy

---

[87] Kent Walker, *The Urgent Necessity of Enacting a National Privacy Law*, GOOGLE: THE KEYWORD (Apr. 25, 2022), https://perma.cc/53BG-6FLZ.

[88] Jedidiah Bracy, *Apple's Tim Cook: Protecting Privacy 'Most Essential Battle of Our Time'*, IAPP: PRIVACY ADVISOR (Apr. 12, 2022), https://perma.cc/3EV6-HW93.

[89] David A. Hoffman, *The U.S. Must Have Strong Enforcement for a Successful Privacy Regime*, INTEL: POLICY@INTEL (May 27, 2019), https://perma.cc/LK6J-YDUV.

[90] *Id.*

[91] *See* U.S. Chamber's Model Data Privacy Legislation, U.S. CHAMBER OF COM. (Feb. 13, 2019), https://perma.cc/D4ZN-5QVZ.

[92] *Id.*

[93] Mark Zuckerberg, *The Internet Needs New Rules. Let's Start in These Four Areas*, WASH. POST (Mar. 30, 2019), https://perma.cc/E942-ZWXJ.

[94] *See, e.g.*, Consumer Online Privacy Rights Act, S. 3195, 117th Cong. (2021); Data Protection Act of 2021. S. 2134, 117th Cong. (2021); Information Transparency & Personal Data Control Act, H.R. 1816, 117th Cong. (2021); Consumer Data Privacy and Security Act of 2021, S. 1494, 117th Cong. (2021); SAFE DATA Act, S. 2499, 117th Cong. (2021).

[95] *Policy Principles for a Federal Data Privacy Framework in the United States Before the S. Comm. on Com., Sci., & Transp.*, 116th Cong. (2019).

[96] *GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation Before the S. Comm. on the Judiciary*, 116th Cong. (2019).

[97] *Protecting Consumer Privacy Before the S. Comm. on Com., Sci, & Transp.*, 117th (2021).

[98] *Statement of Chair Lina M. Khan Regarding the Report to Congress on Privacy and Security Commission* 2–3 (F.T.C. File No. P065401, Oct. 1, 2021), https://perma.cc/WZ6F-VDYJ.

legislation, the United States remains an outlier compared to the over 100 countries that have baseline privacy laws."[99]

2. *Government Access, Use, and Storage of Personal Data*

The U.S. Privacy Act of 1974 laid the foundation for establishing a personal right to data privacy, balancing the government's need for information about individuals with their right to be protected against unwarranted invasions of their privacy stemming from federal agencies' collection, maintenance, use, and disclosure of personal information about them.[100] Enacted in the wake of the Watergate scandal, the law reflects a concern with government abuse, evident in its restriction on disclosure of personal information and the right to access or amend personal records.[101] Consistent with this right to privacy, subsequent federal legislation, including the Foreign Intelligence Surveillance Act of 1978 (FISA)[102] and the Electronic Communications Privacy Act (ECPA),[103] further refined how the government must handle personal digital data in a law enforcement context.

FISA establishes procedures governing electronic surveillance to gather foreign intelligence, including: (1) the creation of a Foreign Intelligence Surveillance Court (FISC) tasked with issuing warrants to authorize surveillance of foreign agents; (2) a record destruction requirement for communications accidentally intercepted; and (3) a limited presidential exception to the FISC warrant requirement.[104]

The ECPA protects a person's oral, electronic, and wire conversations from unauthorized government interception and access through three broad buckets of legislation: (1) the Wiretap Act, which prohibits the intentional interception of wire, oral or electronic communications;[105] (2) the Stored Communications Act, which protects the privacy of records such as subscriber names, billing records, or IP addresses;[106] (3) the Pen Register and Trap and Trace Act, which requires a court order to install a pen register or trap and trace device to monitor telephone communications.[107]

---

[99] Cameron F. Kerry, *One year after Schrems II, the world is still waiting for U.S. privacy legislation*, BROOKINGS TECHTANK (Aug. 16, 2021), https://perma.cc/9XHG-J73J.

[100] *See* Privacy Act of 1974, 5 U.S.C. § 552a.

[101] *See id.* § 552a(b), (d).

[102] Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c.

[103] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–23, 2701–12, 3121–27.

[104] *See* 50 U.S.C. §§ 1801–02, 1806(i). The President's power to bypass surveillance without a FISC warrant exists for up to a year, if the Attorney General certifies there is "no substantial likelihood that the surveillance will acquire the contents of any communication to which a U.S. person is a party," provided the surveillance is directed solely at communications among or between foreign powers, or "the acquisition of technical intelligence . . . from property or premises under the open and exclusive control of a foreign power." 50 U.S.C. § 1802.

[105] 18 U.S.C. § 2515. Title I of ECPA updated the Federal Wiretap Act of 1968, which addressed the interception of conversations using hard telephone lines but did not apply to interceptions of computer, electronic, and other digital communications. *Id.* §§ 2510–22. Exceptions to Title I of the ECPA exist for persons authorized to conduct surveillance as provided under FISA. *Id.* § 2511.

[106] 18 U.S.C. §§ 2701–12.

[107] *See* 18 U.S.C. §§ 3121–27. As with the Wiretap Act, there is an exception for pen registers and trap and trade devices under FISA. *See* 50 U.S.C. § 1802.

3. *Private Access, Use, Sale, and Storage of Personal Data*

As in Russia,[108] federal law also governs how private companies handle personal data, largely on an industry-wide basis. Unlike Russian laws, U.S. law does not typically address things like principles of transparency, limiting the lawful bases for processing, the purpose of the limitation, or data minimization. Rather, U.S. law focuses on a data subject's right to access their data[109] or to opt-out of receiving commercial e-mails or phone calls, which are generated through processing of personal data.[110] The Gramm–Leach–Bliley Act, for example, applies these concepts to banks, insurance companies, and financial service companies in order to govern the protection of Non-Public Personal Information (NPI), including any information collected from customers in connection with the provision of financial services.[111] It imposes requirements for securing, disclosing, and using NPI. As noted above, HIPAA protects personal health information (PHI) and generally regulates the collection and disclosure of PHI under its security privacy rules.[112] The Fair Credit Reporting Act (FCRA) restricts the use of information concerning a person's credit standing, character, general reputation, and mode of living, while still permitting disclosure to entities with a valid need for the information, such as banks, landlords, insurance companies, and potential employers.[113]

The longstanding Federal Trade Commission Act empowers the FTC to protect consumers against unfair or deceptive practices.[114] The law empowers the FTC to enact and enforce federal privacy and data protection regulations related to web-based companies. For example, the FTC has taken the position that a company's failure to comply with its published privacy policies and its failure to adequately secure personal information is a deceptive practice under the Act's definition.[115]

4. *Children's Personal Data*

The FTC is also tasked with enforcing the Children's Online Privacy Protection Act of 1998 (COPPA), which applies to the operator of a website or online service that is "directed to children"[116] and specifically addresses the use, disclosure, and processing of personal information of a child under the age of thirteen.[117] Before any such information can be collected or used, an operator must obtain "verifiable parental consent" in addition to providing parents both access to all information

---

[108] *See infra* Part IV.

[109] *See, e.g.*, 29 U.S.C. § 1181 (subject may request personal health information (PHI) under the Health Information Portability and Accountability Act (HIPAA)); Fair Credit Reporting Act, 15 U.S.C. §§ 1681–81x (subject may receive a copy of consumer credit report).

[110] Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003, 15 U.S.C. §§ 7701–13.

[111] 15 U.S.C. § 6802(a).

[112] 29 U.S.C. § 1181.

[113] 15 U.S.C. § 1681.

[114] 15 U.S.C. §§ 41–58.

[115] 15 U.S.C. § 45; *see also* Fed. Trade Comm'n, 2020 Privacy and Data Security Update (Sept. 13, 2021) https://perma.cc/B9ZM-YHRZ.

[116] *See* 15 U.S.C. §§ 6501 *et. seq.* (1998).

[117] *Id.* § 6501(1).

collected on their child and the right to ask that any of the information be erased.[118] Verifiable parental consent is not required if a child's online contact information is collected on a one-time basis (in response to a specific request from the child and not retained), collected for the sole purpose of obtaining parental contact information to obtain consent, collected and used only to protect the child, or collected to protect the security of the website or respond to judicial process.[119]

The FTC has brought dozens of high-profile suits, with the penalties imposed increasing in size, perhaps signaling an increased attention to COPPA violations. In February of 2019, the FTC settled a COPPA complaint against video social networking app, Musical.ly (now known as TikTok) for $5.7 million.[120] According to FTC Chairman Joe Simons, "[t]he operators of Musical.ly . . . knew many children were using the app but they still failed to seek parental consent before collecting names, email addresses, and other personal information from users under the age of 13."[121] He added that the penalty "should be a reminder to all online services and websites that target children: We take enforcement of COPPA very seriously, and we will not tolerate companies that flagrantly ignore the law."[122] In September of 2021, Google LLC and its subsidiary YouTube LLC agreed to pay a $170 million civil penalty to the Federal Trade Commission and the New York Attorney General to settle allegations that YouTube's video-sharing service illegally collected personal information from children without their parent's consent in violation of COPPA. Recent COPPA actions have been less extreme, with a $3 million settlement and permanent injunction issued against KuuHuub due to its failure to provide sufficient notice of the information it collects from children (or to obtain verifiable parental consent).[123]

5. *Artificial Intelligence*

Unlike in Russia, which has enacted an experimental regime to govern artificial intelligence (AI),[124] no general regulatory framework on AI currently exists in the U.S. The White House Office of Science and Technology Policy has put forth ten principles to consider when formulating regulatory and non-regulatory approaches to the development and use of AI.[125] Although there is limited case law or

---

[118] *Id.* §§ 6501(9), 6502(b).

[119] *Id.* § 6502(b).

[120] *Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law*, FEDERAL TRADE COMMISSION (Feb. 27, 2019), https://perma.cc/5DQL-CQAR.

[121] *Id.*

[122] *Id.*

[123] The FTC has provided a safe harbor or "pre-approval" under COPPA for those who agree to self-regulate. Companies that have taken advantage of this safe harbor include Children's Advertising Review Unit (TV and radio advertisers), iKeepSafe (children's educational technology group), kidSAFE (programmer for preschool and elementary schools), Privacy Vaults Online, Inc. (compliance organization for online companies) and TRUSTe (compliance and security company). Aristotle International Inc. (political campaign data aggregators), one of the first companies to obtain the safe harbor, was recently removed from the list by the FTC for failure to monitor affiliated companies. Peder Magee, *Aristotle Removed from List of FTC-Approved Children's Privacy Self-Regulatory Programs*, FEDERAL TRADE COMMISSION (Aug. 4, 2021), https://perma.cc/MY3F-XNRM.

[124] *See infra* Part IV.2.

[125] (1) Public trust in AI; (2) Public Participation; (3) Scientific Integrity and Information Quality; (4) Risk Assessment and Management; (5) Benefits and Costs; (6) Flexibility; (7) Fairness and Non-

regulation in the U.S. covering privacy as related to AI, Congress continues to consider legislation aimed at privacy and AI, including the Facial Recognition and Biometric Technology Moratorium Act;[126] the Algorithmic Justice and Online Platform Transparency Act (S. 1896);[127] and the Data Protection Act of 2021.[128]

In February 2020, the Electronic Privacy Information Center (EPIC) petitioned the FTC to develop rules concerning the use of AI in commerce in order to protect consumers from harm caused by AI products.[129] In April 2021, the FTC published guidance regarding the commercial use of AI technology, urging companies to be transparent with consumers, explain how algorithms make decisions, and ensure that decisions are fair, robust, and empirically sound.[130]

On January 11, 2021, the FTC ordered AI company Everalbum, Inc. to delete or destroy any machine learning models or other algorithms developed using biometric information it unlawfully collected from users, along with the biometric

---

Discrimination; (8) Disclosure and Transparency; (9) Safety and Security; and (10) Interagency Coordination. OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, M-21-06, MEMORANDUM ON GUIDANCE FOR REGULATION OF ARTIFICIAL INTELLIGENCE APPLICATIONS (2002), https://perma.cc/54AQ-MLQL.

[126] Facial Recognition and Biometric Technology Moratorium Act of 2021, S. 2052, 117th Cong. (2021). On June 15, 2021, Senators Edward Markey (D-Mass.), Jeff Merkley (D-Ore.), Bernie Sanders (I-Vt.), Elizabeth Warren (D-Mass.), and Ron Wyden (D-Ore.) reintroduced the Facial Recognition and Biometric Technology Moratorium Act, which would prohibit government agencies from using facial recognition technology and other biometric surveillance—including voice recognition, gait recognition, and recognition of other immutable physical characteristics—by state and federal entities, and block federal funds for biometric surveillance systems. The legislation, which is endorsed by the ACLU and numerous other civil rights organizations, also provides a private right of action for individuals whose biometric data is used in violation of the Act (which can also be enforced by state attorneys general) and seeks to limit local entities' use of biometric technologies by tying receipt of federal grant funding to localized bans on biometric technology. Any biometric data collected in violation of the bill's provisions would also be banned from use in federal judicial proceedings).

[127] Algorithmic Justice and Online Platform Transparency Act, S. 1896, 117th Cong. (2021); *see also* Press Release, *Senator Markey, Rep. Matsui Introduce Legislation to Combat Harmful Algorithms and Create New Online Transparency Regime*, U.S. SENATOR ED MARKEY OF MASSACHUSETTS (2021), https://perma.cc/2GR8-67PY. On May 27, 2021, Senator Edward J. Markey (D-Mass.) and Congresswoman Doris Matsui (CA-06) introduced the Algorithmic Justice and Online Platform Transparency Act of 2021 to prohibit harmful algorithms, increase transparency into websites' content amplification and moderation practices, and commission a cross-government investigation into discriminatory algorithmic processes across the national economy. The Act would prohibit algorithmic processes on online platforms that discriminate on the basis of race, age, gender, ability, and other protected characteristics. In addition, it would establish a safety and effectiveness standard for algorithms and require online platforms to describe algorithmic processes in plain language to users and maintain detailed records of these processes for review by the FTC. Press Release, *Senator Markey, Rep. Matsui Introduce Legislation to Combat Harmful Algorithms and Create New Online Transparency Regime*, U.S. SENATOR ED MARKEY OF MASSACHUSETTS (2021), https://perma.cc/2GR8-67PY.

[128] Data Protection Act, S. 2134, 117th Cong., §§ 2(3), (11)-(13) (2021). As noted above, the Data Protection Act would create an independent federal agency to protect consumer data and privacy. The main focus of the agency would be to protect individuals' privacy related to the collection, use, and processing of personal data. The bill defines an "automated decisions system" as "a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision, or facilitates human decision making." *Id.* Moreover, using "automated decision system processing" is a "high-risk data practice" requiring an impact evaluation after deployment and a risk assessment on the system's development and design, including a detailed description of the practice including design, methodology, training data, and purpose, as well as any disparate impacts and privacy harms. *Id.*

[129] *EPIC Seeks Regulation of AI, Petitions Federal Trade Commission*, EPIC (Feb. 3, 2020), https://perma.cc/UC3W-T7NE.

[130] Elisa Jillson, *Aiming for truth, fairness, and equity in your company's use of* AI, FEDERAL TRADE COMMISSION: BUSINESS BLOG (Apr. 19, 2021), https://perma.cc/Y8B7-KH5F.

data itself.[131] As noted above, although no cases have yet resolved the issue, the GDPR standards will likely affect AI companies doing business in the European Union. For example, Article 22 states that a data subject shall have the right "not to be subject to a decision based solely on automated processing" unless certain permitted conditions (such as express and informed consent) are present.[132]

6. *Big Data*

Likewise, several federal regulations impact—albeit without specifically addressing—Big Data in the privacy context.[133] HIPAA and the FCRA impact the access, use, and storage of PHI and consumer credit records.[134] Similarly, the Family Educational Rights and Privacy Act of 1974 (FERPA) regulates the privacy records of students in schools and places limitations on data that can be obtained and used by third parties.[135] While federal statutes like HIPAA and FERPA regulate certain types of data, federal law surrounding Big Data goes further than regulating its mere collection. In 2016, the FTC issued a report on Big Data that said its use had the potential to harm low-income and "underserved communities" because it could be used to exclude those communities from "credit and employment opportunities."[136] The FTC

---

[131] Everalbum, Inc., F.T.C., 4–5 (2021), https://perma.cc/XLZ9-E4VZ.

[132] General Data Protection Regulation, *supra* note 1, art. 22.

[133] *See* "big data, C2, 23." *OED Online*, Oxford University Press, March 2022, https://perma.cc/MK69-7LAG (defining "big data" as: "data of a very large size, typically to the extent that its manipulation and management present significant logistical challenges."). The term first gained traction in 2001 when industry analyst Doug Laney coined Big Data as having the three V's (volume, velocity, and variety). G. Piatestsky, *Exclusive Interview: Doug Laney on Big Data and Infonomics*, KDNUGGETS.COM (Jan. 15, 2018), https://perma.cc/5SYF-D966. Big Data can either be created by people or generated by machines, such as sensors gathering climate information, satellite imagery, digital pictures and videos, purchase transaction records, GPS signals, etc., and can cover many sectors, from healthcare to transport and energy. *BIG DATA*, EUROPEAN COMMISSION: SHAPING EUROPE'S DIGITAL FUTURE (Feb. 24, 2022), https://perma.cc/9T5G-5AQ4.

[134] Health Insurance Portability and Accountability Act, 29 U.S.C. § 1181; Fair Credit Reporting Act, 15 U.S.C. § 1681. A hurdle to bringing actions in federal court under some of these federal laws by private individuals is the constitutional concept of standing. In June of 2021, the Supreme Court in *TransUnion v. Ramirez* addressed the issue in the context of the Fair Credit Reporting Act. *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2210–12 (2021). In *TransUnion*, the Court held that only a fraction of the class members whose inaccurate credit reports were sent to potential creditors suffered any actual, concrete harm. *Id.* Although other plaintiffs had inaccurate reporting included on their TransUnion credit reports, those inaccurate reports were not disseminated. *Id.* at 2099. The *TransUnion* case suggests that plaintiffs who allege mere violations of data privacy laws may not have standing to sue unless they can show they have suffered a "concrete harm" (such as use, copying, or access by a third party) as a result of the violation, and does little to resolve a split among lower federal courts concerning whether disclosure of personal information alone amounts to a data privacy violation. *Id.* at 2211. *See also Blahous v. Sarrell Reg'l Dental Center for Pub. Health, Inc.*, 2:19-CV-798-RAH-SMD, 2020 WL 4016246, at *14–16 (M.D. Ala. July 16, 2020) (disclosing personal information was not sufficient to confer class standing since there was no evidence that any breached files were copied, downloaded, or otherwise removed); *Antman v. Uber Techs., Inc.*, 15-CV-01175-LB, 2018 WL 2151231, at *12–13, n.55 (N.D. Cal. May 10, 2018) (hacking information such as social security numbers would create injury sufficient to support standing to sue for data privacy breach); *Hartigan v. Macy's, Inc.*, 501 F. Supp. 3d 1, 5–6 (D. Mass. 2020) (dismissing data privacy claim because (1) plaintiff did not allege fraudulent use or attempted use of his personal information to commit identify theft; (2) the stolen information "was not highly sensitive or immutable like social security numbers"; and (3) immediately cancelling a disclosed credit card can eliminate the risk of future fraud.).

[135] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(g).

[136] FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION 9–10 (2016).

noted that organizations using Big Data needed to be aware of the regulatory limits that are in place, such as the FCRA, the FTCA, and equal opportunity laws.[137]

More recently, Congress has held hearings on the use of Big Data in the context of the COVID-19 pandemic.[138] The Senate Committee on Commerce, Science, and Transportation said it would "examine recent uses of aggregate and anonymized consumer data to identify potential hotspots of coronavirus transmission and to help accelerate the development of treatments."[139] The Committee stated it would "also examine how consumers' privacy rights are being protected and what the U.S. government plans to do with COVID-related data collected at the end of this national emergency."[140]

Since the start of the COVID-19 outbreak, EPIC has worked with technology experts, legal scholars, NGOs, public health officials, data protection authorities, human rights experts, and international organizations to promote an effective response to the pandemic that still protects privacy. EPIC's key recommendations include:

> (1) [A] fundamental emphasis on effective public health measures and evidence-based policy, (2) strong enforcement of privacy obligation and robust techniques for deidentification, (3) new accountability measures for data uses and due process safeguard[s], and (4) avoidance of a centralized system of mass surveillance that will be difficult to dismantle after the pandemic.[141]

EPIC President Marc Rotenberg recently told Buzzfeed, "People say, 'well, we need to strike a balance between protecting public health and safeguarding privacy' — but that is genuinely the wrong way to think about it. You really want both. And if you're not getting both, there's a problem with the policy proposal."[142]

One federal statute, the Computer Fraud and Abuse Act (CFAA), may be interpreted to prohibit web scraping, or the automated gathering of Big Data from a third-party website. The CFAA protects computers and computer systems from unauthorized access.[143] In the case *hiQ Labs v. LinkedIn Corp.*, one Federal Circuit Court initially held that the common practice of website scraping does not violate the CFAA because the data that hiQ scraped was already available to anyone with a web

---

[137] *Id.* 12–23.

[138] Press Releases, *Committee Announces Paper Hearing on Big Data and the Coronavirus*, U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION (Apr. 2, 2020), https://perma.cc/8REA-QQVU.

[139] *Id.*

[140] *Id.*

[141] *Big Data and the Future of Privacy*, ELEC. PRIV. INFO. CTR, https://archive.epic.org/privacy/big-data/ (last visited May 5, 2022).

[142] Rosie Gray & Caroline Haskins, *The Coronavirus Pandemic Has Set Off a Massive Expansion of Government Surveillance. Civil Libertarians Aren't Sure What to Do*, BUZZFEED NEWS (Apr. 3, 2020), https://perma.cc/4LY5-HWZH

[143] Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(a)(2) (prohibiting individuals from "access[ing] a computer . . . without authorization.").

browser and thus not a violation of LinkedIn's website terms.[144] Scraping data may, however, violate other U.S. laws concerning copyright, contract, and tort law.[145]

C. State Regulations

Many states have laws protecting the personal data of their residents, but California, Colorado, and Virginia are currently the only that have enacted comprehensive data privacy laws. California's Privacy Rights Act (CPRA) of 2020 is the most comprehensive privacy statute enacted to date, adopting an approach similar to the GDPR.[146] CPRA expands the California Consumer Privacy Act (CCPA), which was been adopted in 2018, and will become fully operational on January 1, 2023, as will the Colorado and Virginia statutes.[147]

In most regards, the California, Colorado, and Virginia frameworks are similar to the GDPR. Like the GDPR, these statutes protect personal information that relates to an individual, as well as information specific to a device or an entire household.[148] Similarly, they all allow a business to collect, use, sell, or disclose information that is aggregated or anonymized and generally require businesses to implement security measures to protect against data breaches (although without providing explicit security requirements).[149] All three state statutes also allow data subjects a similar right to access their personal information and to request that data be transferred to another controller (a concept known as data portability).[150]

While the GDPR, Colorado, and Virginia laws generally use the terms "controller" or "processor,"[151] California law refers to "businesses" and "service providers."[152] These terms have similar, but not identical, meanings. For example, in order to qualify as a "business" under California law, an entity must "determine[] the purposes and means of the processing of consumers' personal information"—language that mirrors the GDPR's definition of a controller.[153] Similarly, in order to qualify as

---

[144] *hiQ Labs v. LinkedIn Corp.*, 938 F.3d 985, 991 (9th Cir. 2019), *vacated*, 141 S. Ct. 2752 (2021), *remanded to* 31 F.4th 1180 (2022) for further consideration in light of *Van Buren* v. *United States*, 141 S.Ct. 1648 (2021).

[145] *See, e.g.*, *WhatsApp Inc. v. NSO Group Technologies Ltd.*, 472 F. Supp. 3d 649 (N.D. Cal., 2020) (CFAA cause of action for digital breaking and entering is a trespass offense).

[146] Cal. Civ. Code §§ 1798.100 *et seq*. *See also* Colorado Privacy Act, S.B. 21-190 (Colorado Privacy Act), 73d Leg. Reg. Sess. (Colo. 2021) (to be codified in Colo. Rev. Stat. §§ 6-1-1301 *et seq*.) (effective July 1, 2023); Virginia Consumer Data Protection Act, codified in Va. Code Ann. § 59.1-576.

[147] Cal. Civ. Code § 1798.100 *et seq*. (2020).

[148] *See, e.g.*, Cal. Civ. Code §§ 1798.140(o), 1798.145(c)–(f) (2020); Cal. Code Regs. tit. 18, §17014; Va. Code Ann. §§ 59.1–571; Col. Rev. Stat. § 6-1-1303(6); *see also* General Data Protection Regulation, *supra* note 1, arts. 4(1), 9(1).

[149] *See, e.g.*, Cal. Civ. Code §§ 1798.140(a), (h), (o), (r); 1798.145(a)(5). Cal. Civ. Code § 1798.150(a)(1); Va. Code Ann., §§ 59.1–574(A)(3), 59.1–574(D), 59.1–575(A)(2); Col. Rev. Stat. §§ 6-1-1304(3)(a)(X), 6-1-1305(2)(b), 6-1-305(4), 6-1-1308(5); General Data Protection Regulation, *supra* note 1, art. 24(1).

[150] Cal. Civ. Code §§ 1798.100(d), 1798.110, 1798.115, 1798.125(b)(3); Va. Code Ann., §§ 59.1-573(A)(4); Col. Rev. Stat. §§ 6-1-1306(1)(e); General Data Protection Regulation, *supra* note 1, art. 15. *See also* Cal. Civ. Code §§ 1798.100(d), 1798.130(a)(2); General Data Protection Regulation, art. 20.

[151] *See* Va. Code Ann. § 59.1-571; Col. Rev. Stat. § 6-1-1301. General Data Protection Regulation, *supra* note 1, art. 4(7).

[152] Cal. Civ. Code §1798.140(v).

[153] *Id.* §1798.140.

a "service provider" under California law, an entity must, in part, "process information on behalf of a business."[154]

Whether a company fits the definition of a "business" is not always straightforward. The analysis is fact driven and can depend upon a variety of factors, including:

- What personal data will be collected?
- What will the personal data be used for?
- How long will the personal data be stored?
- Who will have access to the personal data (within or outside of the company)?

In some ways, the California, Colorado, and Virginia laws are narrower in scope than the GDPR. For example, unlike the GDPR, the California and Virginia laws apply only to "for profit entities."[155] California narrows its application further to only cover entities that (1) have gross annual revenue of over $25M, (2) control or process the data of over 50,000 consumers (over 100,000 as of January 1, 2023), or (3) derive at least 50% of its revenue from the sale of personal data.[156] The Colorado and Virginia laws have no minimum revenue threshold criteria, but they do apply only to businesses that control or process the data of (1) over 100,000 consumers, or (2) over 25,000 users if (in Virginia) the business derives at least 50% of its revenue from the sale of personal data, or if (in Colorado) the business derives some revenue or receive a discount on the price of goods or services resulting from the sale of personal data.[157] Yet, like the GDPR, California, Colorado, and Virginia require that businesses disclose to data subjects what information is collected and how it is used.[158]

Unlike the GDPR, the California, Colorado, and Virginia laws require businesses to give data subjects explicit notice (and an opportunity to "opt out") before re-selling personal information.[159] In California, that notice requirement extends only to the twelve months preceding any request (after which a business can ask a consumer to "opt in").[160] Unlike Colorado and Virginia, however, California requires a "Do Not Sell My Personal Information" link be clearly and conspicuously displayed on a business homepage.[161] The CPRA extends the "opt out" requirement to include profiling (or automated decision-making) and mandates an additional "Limit the Use of My Sensitive Personal Data" link.[162] Beginning July 1, 2024, Colorado will also require a universal opt-out mechanism for consumers, although the exact format of

---

[154] *Id.*

[155] Cal. Civ. Code § 1798.140(c); Va. Code Ann. §§ 59.1-572(B)(iv).

[156] Cal. Civ. Code § 1798.140(c).

[157] Va. Code Ann. §§ 59.1-572(A)(i), (ii); Col. Rev. Stat. § 6-1-1304(b)(I)–(II).

[158] Cal. Civ. Code §§ 1798.100(a)–(b), 1798.105(b), 1798.110, 1798.115, 1798.120(b), 1798.130, 1798.135; Va. Code Ann. §§ 59.1-574; Col. Rev. Stat. § 6-1-1308.

[159] Cal. Civ. Code §§ 1798.120, 1798.125(b)(3); Va. Code Ann., § 59.1-573; Col. Rev. Stat. § 6-1-1308(1)(a)(V)(b).

[160] Cal. Civ. Code §§ 1798.120, 1798.125(b)(3).

[161] Cal. Civ. Code §§ 1798.120, 1798.135(a)–(b).

[162] *Id.* § 1798.185(a)(19)(A).

such a mechanism is not specified.[163] The GDPR does not require an "opt out" for selling data but does include a provision allowing a data subject to opt out of data processing done for marketing purposes.[164] The GDPR also provides data subjects broad rights to object to processing or automated decision-making, such as for profiling, marketing, statistical, or scientific purposes; California's CPRA does not allow for these types of subject-matter specific objections.[165]

All statutes impose requirements for processing a child's personal information (children being those under the age of thirteen for the purposes of the California, Colorado, and Virginia laws,[166] and those under the age of sixteen for the GDPR). However, the U.S. laws require parental consent only for the sale of personal information, whereas the GDPR's parental consent requirements extend to *all* types of data processing for children's information.[167]

Finally, the private right of action and damages available to individuals vary under these laws. California law establishes a limited private right of action for breaches but gives a company a 30-day "cure period" (which will be eliminated as of January 2023), with penalties of $100 to $750 per consumer, and an automatic $7,000 civil fine per violation involving the personal information of a minor.[168] By contrast, Virginia law establishes civil penalties of up to $7,500 per violation, but no private right of action.[169] Similarly, no private right of action exists under Colorado law, with the Attorney General exclusively empowered to seek injunctive relief for violations.[170] The GDPR provides a broader private right of action for material and non-material damages, with penalties calculated at either €20,000,000 or 4% of a company's annual global revenue (whichever is higher).[171]

IV. Russian Data Privacy Regulations

Data privacy in Russia is an evolving area of law experiencing rapid change. The key regulations governing data privacy are the Russian Constitution, various federal laws and regulations, and international treaties.

A. Russian Constitution

Unlike the United States Constitution, the Russian Constitution explicitly states that citizens have a right to privacy. More specifically, the Russian Constitution provides that "[t]he collection, keeping, use and dissemination of information about

---

[163] Col. Rev. Stat. §§ 6-1306(1)(a)(IV)(B), 6-1-1313 (explaining opt-out messages must be consumer-friendly).

[164] General Data Protection Regulation, *supra* note 1, art. 21.

[165] *Id.* arts. 21–22.

[166] The state requirements concerning use and disclosure of information for children under 13 do not override the federal protections of COPPA. 15 U.S.C. §§ 6501 *et seq.* Va. Code Ann., §§ 59.1-572(D), 59.1-574(A)(5); Col. Rev. Stat. §§ 6-1-1304(2)(j)(IV).

[167] Cal. Civ. Code §§ 1798.120(c)-(d); Va. Code Ann. §§ 59.1-571(A), 59.1-574(A)(5); Col. Rev. Stat. §§ 6-1-1304(1)(b), 6-1-1308(7); General Data Protection Regulation, *supra* note 1, art. 8(1).

[168] Cal. Civ. Code §§ 1798.150, 1798.155.

[169] Va. Code Ann., §§ 59.1-580(C), 591-580 (E).

[170] Col. Rev. Stat. § 6-1-1311.

[171] General Data Protection Regulation, *supra* note 1, arts. 82–84.

the private life of a person shall not be allowed without his or her consent," and that officials representing "bodies of state authority and local self-government . . . shall ensure for everyone the possibility of acquainting [sic] with the documents and materials directly affecting his or her rights and freedoms, unless otherwise provided for by law."[172] It further holds that "[t]he home shall be inviolable. No one shall have the right to get into a house against the will of those living there, except for the cases established by a federal law or by court decision."[173]

B. General Privacy Regulation

Russian Federal Law No. 149-FZ on Information, Information Technologies, and the Protection of Information regulates public relations in connection with the circulation of information in Russia.[174] Article 5 of this law divides information into four categories: (1) information freely disseminated; (2) information obtained with consent; (3) information provided in accordance with federal laws; and (4) information prohibited for distribution in the Russian Federation.[175]

Russian Federal Law No. 152-FZ on Personal Data forms the framework for personal data protection in Russia, regulating personal data processing carried out by operators.[176]

Article 3 of No. 152-FZ defines personal data as "any information referring directly or indirectly to a particular or identified individual (hereinafter referred to as 'personal data subject')."[177] Article 5 addresses further key principles relevant to the processing of personal data, including the purpose for processing the data (i.e., legality and good faith), the operator's authority to process the data, the volume and nature of the data processed, and the reliability and sufficiency of the data processed.[178]

Article 3 defines an operator as a "state agency, municipal authority, legal entity or individual who independently or in cooperation with other entities organizes and/or processes personal data."[179] An operator also determines the purposes of processing personal data, the composition of personal data to be processed, and the actions (operations) performed with personal data.[180] This definition under Russian law embraces both GDPR concepts of "processor" (processing) and "controller" (organizing). No. 152-FZ allows operators to search or access personal data fixed on

---

[172] KONSTITUTSIIA ROSSIĬSKOĬ FEDERATSII [KONST. RF] [CONSTITUTION] art. 24, https://perma.cc/9RUK-68W6.

[173] *Id.* art. 25.

[174] Federal'nyĭ Zakon RF No. 149-FZ ob Informatsii, Informatsionnykh Tekhnologiiakh i o Zaschite Informatsii, [Russian Federation Collection of Legislation], SOBRANIE ZAKONODATEL'STVA ROSSIĬSKOĬ FEDERATSII [SZ RF] 2006, No. 31, Item 3448, http://www.consultant.ru/document/cons_doc_LAW_61798/ (last visited June 26, 2022).

[175] *Id.* art. 5.

[176] Federal'nyĭ Zakon RF No. 152-FZ o Personal'nykh Dannykh [Federal Law of the Russian Federation on Personal Data], SZ RF 2006, No. 31, Item 3451, https://perma.cc/QWX4-VKJW.

[177] *Id.* art. 3.

[178] *Id.* art. 5.

[179] *Id.* art. 3.

[180] *Id.*

some material object and stored in files or in some other way.[181] It does not cover personal data processing by physical persons for personal and family purposes (when it does not infringe on the rights of personal data subjects).[182] Nor does it cover the organization of storage, integration, accounting, and use of the documents of the Archive Fund of the Russian Federation and other archive documents containing personal data (when done in accordance with the Russian Federation archiving legislation)[183] or the processing of personal data containing state secrets.[184]

Article 6 specifies that an operator may only process personal data with the consent of the subject of that data.[185] However, such consent is not required if it is prescribed by international agreement or federal law; is done for the purposes of performing a contract if the subject is a party to that contract; for judicial, statistical, scientific, literary, or other creative purposes subject to de-personalization of the data; for protection of life, health, and vital interests of the subject if it is impossible to obtain their consent; or for professional media activity.[186]

Furthermore, under Article 22 of Federal Law No. 152-FZ, before processing personal data, all operators "shall be obliged to notify the authorized body for the protection of data subjects of its intention to . . . carry out the processing of personal data."[187] The authorized body is the Roskomnadzor, Russia's federal agency regulating data protection for telecommunications, information technologies, and mass communications companies.

An operator has the right to process personal data without notifying the authorized body, in this case the Roskomnadzor, if such data is processed in accordance with labor laws; is received by the operator by concluding a contract to which the subject of personal data is a party; is processed for the purposes of public associations or religious organizations; is published by the data subject; includes only the surnames, names and patronymics of the data subject; is necessary for the one-off admission of the data subject onto premises where the operator is situated; is included in state automated information systems; is included in state personal data filing systems created for state security and public order; is processed without the use of automated services; or is processed for transport security.[188] Barring any of the foregoing exceptions, the operator's notification to the Roskomnadzor:

> [S]hall be sent in the form of a paper document or in the form of an electronic document and shall be signed by an authorized person. The notification shall contain the following information: (1) the name (surname, first name, and patronymic) and address of the operator; (2) the purpose of the processing of personal data; (3) the categories of personal data; (4) the categories of data subjects whose personal data are to be processed; (5) the legal basis of the

---

[181] *Id.*

[182] *See id.*

[183] Federal'nyĭ Zakon RF No. 125-FZ ob Arkhivnom Dele v RF [Russian Federal Law No. 125-FZ on Archiving in the Russian Federation], SZ RF 2004, No. 43, Item 4169, http://www.consultant.ru/document/cons_doc_LAW_1406/ (last visited June 26, 2022).

[184] Russian Federal Law No. 152-FZ, art. 3.

[185] *Id.* art. 6.

[186] *Id.*

[187] *Id.* art. 22.

[188] *Id.*

> processing of personal data; (6) a list of actions to be performed in relation to personal data and a general description of the methods of processing personal data which are to be used by the operator. . .; (7.1) the surname, first name and patronymic of the physical person or the name of the organization responsible for organizing the processing of personal data, and their contact telephone numbers, postal addresses and electronic mail addresses; (8) the date on which the processing of personal data is to begin; (9) the period or condition of termination of the processing of personal data; (10) information on whether or not the cross-border transfer of personal data occurs in the course of the processing of personal data; (11) information on measures taken to ensure the security of personal data in accordance with requirements established by the Government of the Russian Federation for the protection of personal data.[189]

Russian Federal Law No, 242-FZ on Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunications Networks[190] amends Article 18 of Federal Law No. 152-FZ by adding requirements for the localization of personal data:

> During personal data collection, inter alia, through the Internet, the operator shall ensure that databases located within the Russian Federation are used to record, systematize, accumulate, store, clarify (update or modify) and retrieve personal data of citizens of the Russian Federation.[191]

This law generally applies to Russian companies as well as foreign companies that have presence in Russia.

Like the GDPR, Federal Law No. 242-FZ might apply to foreign companies without a legal presence in Russia if the operators' platforms seem sufficiently oriented toward Russia. This would mirror Russia's approach to conflicts of law regulation for international consumer agreements, which requires applying the law of the consumer's country under Article 1212 of the Russian Civil Code.[192] An operator's Russian orientation can be proved by Russian domain names such as .ru or .rf, websites written in Russian, advertisements in Russian, payment options in Russian currency, delivery options to Russia, and other factors.[193]

As discussed above, Article 22 of 152-FZ requires all operators to inform Roskomnadzor of its intent to process personal data through a notification that "shall be sent in the form of a paper document or in the form of an electronic document and

---

[189] *Id.*

[190] Federal'nyĭ Zakon RF No. 242-FZ o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty Rossiĭskoĭ Federatsii v Chasti Utochneniia Poriadka Obrabotki Personal'nykh Dannykh v Informatsionno-Telekommunikatsionnykh Setiakh, [Amending Some Legislative Acts of the Russian Federation as It Concerns Updating the Procedure for Personal Data Processing in Information Telecommunication Networks], SZ RF 2014, No. 30, Item 4243, https://perma.cc/BY5Z-GG2L.

[191] *Id.* art. 2.

[192] GRAZHDANSKIĬ KODEKS ROSSIĬSKOĬ FEDERATSII [GK RF] [Civil Code] art. 1212, https://perma.cc/52UD-VJK4.

[193] Roskomnadzor Comment to Federal'nyĭ Zakon RF No. 242-FZ at 15.

shall be signed by an authorized person.[194] The notice (among other things) must contain information on whether or not the cross-border transfer of personal data occurs in the course of the processing of personal data."[195]

C. Industry-Specific Laws

Like in the U.S., more detailed privacy laws in Russia relate to specific industries. For example, Chapter 14 of the Russian Labor Code guarantees protection of personal data for employees.[196] Article 86 stipulates that "all personal information of an employee can be received only directly from the employee.[197] If personal information of an employee can be only received from a third party, then the employee must be notified of it in advance and written permission of the employee is required. The employer must inform the employee about purpose, possible sources and means of receiving personal information . . . and consequences of refusal of the employee to provide a written permission on receiving of necessary personal information."[198]

Article 152.2 of the Russian Civil Code guarantees protection of private life.[199] It stipulates that "[e]xcept as otherwise provided by law, it is hereby prohibited without the consent of a citizen the gathering, storage, dissemination and use of any information about his private life, for instance information concerning his origin, whereabouts or place of residence, private and family life."[200] Creation and distribution of works of science, literature, and art that invade the private life of a citizen is prohibited.[201]

Russian Federal Law No. 38-FZ on advertisement (signed into law on March 13, 2006) regulates marketing communications sent by electronic means.[202]

1. Healthcare

In accordance with Article 13 of Russia's core healthcare privacy legislation, information on the nature of medical assistance, health statuses, diagnoses, and other information obtained during medical examination and treatment warrant medical confidentiality and cannot be disclosed.[203] Upon written consent of a patient or his

---

[194] Russian Federal Law No. 152-FZ, art. 22.

[195] *Id.*

[196] TRUDOVOĬ KODEKS ROSSIĬSKOĬ FEDERATSII [TK RF] [Labor Code] art. 86, https://perma.cc/KSF2-UDHP.

[197] *Id.*

[198] *Id.*

[199] Russian Civil Code, art. 152.2, https://perma.cc/WN8K-N36F.

[200] *Id.*

[201] *Id.*

[202] Federal'nyĭ Zakon RF No. 38-FZ o Reklame [Federal Law on Advertisements], SZ RF 2014, No. 12, Item 1232, http://www.consultant.ru/document/cons_doc_LAW_58968/ (last visited June 26, 2022).

[203] Federal'nyĭ Zakon RF No. 323-FZ ob Osnovakh Okhrany Zdorov'ia Grazhdan v Rossiĭskoĭ Federatsii [Russian Federal Law No. 323-FZ on the Basics of Protecting the Health of Citizens in the Russian Federation], SZ RF 2011, No. 48, Item 6724, https://www.ilo.org/dyn/natlex/natlex4.detail?p_isn=102297&p_lang=en (last visited June 26, 2022).

legal representative, this information can be disclosed for the purpose of medical examination, treatment of the patient, conducting scientific research, publishing in academic journals, education, and other purposes.[204]

Article 36.2 of Russia's healthcare technology law mandates that the use of telemedicine technologies in the provision of medical care be carried out in compliance with the requirements established by the legislation of the Russian Federation in the field of personal data and medical confidentiality.[205]

We expect that many governments—including Russia's—will elaborate on the balance between public safety and personal rights and generate new approaches to sharing healthcare data once the COVID-19 pandemic has passed.

2. *Artificial Intelligence*

The first law on artificial intelligence in Russia (No 123-FZ) amended multiple provisions of the existing Russian Federal Law on Personal Data (No. 152-FZ).[206] Article 2 of No. 123-FZ defines artificial intelligence as a complex of technological solutions with which to simulate human cognitive functions (including self-learning and finding solutions without a predetermined algorithm) that leads to results when performing specific tasks that are comparable, at least, to the results of human intellectual activity.[207] This definition encompasses "information and communication infrastructure (including information systems, information and telecommunication networks, other technical means of information processing), software (including [those] using machine learning methods), processes and services for data processing and finding solutions."[208]

An experimental legal regime was established in Moscow for a period of five years starting July 1, 2020.[209] Among the goals of this experiment (defined in Article 3 of Federal Law No. 123-FZ) are life quality improvement; increasing the efficiency of state or municipal government; more efficient implementation of artificial intelligence technologies by businesses; development of an integrated social and legal system for the use of artificial intelligence technologies; testing the impact

---

[204] *Id.*

[205] Federal'nyĭ Zakon RF No. 242-FZ o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty Rossiĭskoĭ Federatsii po Voprosam Primeneniia Informatsionnykh Tekhnologiĭ v Sfere Okhrany Zdorov'ia [Russian Federal Law No. 242-FZ on Amending Certain Legislative Acts of the Russian Federation as to the Implementation of Informational Technology in Healthcare], SZ RF 2017, No. 31, Item 4791, Art. 36.2. http://www.consultant.ru/document/cons_doc_LAW_221184/30b3f8c55f65557c253227a65b908cc075cc114a/ (last visited June 26, 2022).

[206] Federal'nyĭ Zakon RF No. 123-FZ o Provedenii Èksperimenta po Ustanovleniiu Spetsial'nogo Regulirovaniia v Tseliakh Sozdaniia Neobkhodimykh Usloviĭ Dlia Razrabotki i Vnedreniia Tekhnologiĭ Iskusstvennogo Intellekta v Sub"ekte Rossiĭskoĭ Federatsii - Gorode Federal'nogo Znacheniia Moskve» i Vnesenii Izmeneniĭ v Stat'i 6 i 10 Federal'nogo Zakona o Personal'nykh Dannykh [Russian Federal Law No. 123-FZ on Conducting an Experiment to Establish Special Regulation in Order to Create the Necessary Conditions for the Development and Implementation of Artificial Intelligence Technologies in the Subject of the Russian Federation - the City of Federal Significance Being Moscow and Amending Articles 6 and 10 of the Federal Law on Personal Data], SZ RF 2020, No. 17, Item 2701, http://www.consultant.ru/document/cons_doc_LAW_351127/ (last visited June 26, 2022).

[207] *Id.* art. 2(2).

[208] *Id.*

[209] *Id.* art. 1.

of artificial intelligence technologies in Moscow; and the assessment of the efficiency and efficacy of such an experimental legal regime with a view to potentially establishing a special regulation for AI.[210]

Moreover, Article 7 of this law amended Articles 6 and 10 of Russian Federal Law No. 152-FZ on Personal Data to state that "the processing of personal data obtained as a result of depersonalization of personal data is carried out in order to improve the efficiency of state or municipal administration, as well as for other purposes" stipulated by experimental legal regime found in Federal Law No. 123-FZ Article 3.[211]

Under this experimental regime, the Moscow government is entitled to determine the conditions and procedures for development and implementation of AI technologies, as well as procedures for applying the results.[212] Participants of this experiment can be legal entities or individual entrepreneurs registered in Moscow who are carrying out or planning to carry out activities to develop, create, implement, or market artificial intelligence technologies.[213] The law also created a Coordinating Council to formulate strategic directions and monitor the experiment.[214] Based on the results of the experiment, the Coordinating Council will have to submit proposals to the Government of the Russian Federation on appropriate amendments to existing legislation.[215]

3. Big Data

In Russia, no legislation has yet been enacted to address Big Data privacy (particularly in the social media context). This has led to some high-profile judicial rulings, with more expected on the subject. In January 2017, for example, Russian social network VKontakte brought a lawsuit against Double Data, LLC and the National Agency of Credit History alleging that both entities improperly used data from personal VKontakte profiles for assessing the credit risks of potential clients.[216] The Arbitration Court of Moscow initially dismissed the case, basing its decision on the fact that Vkontakte's "database" had limited access, both at the database management system and network levels.[217] Therefore, it was impossible for third parties to access the database and copy its content as a technical matter.[218] However, the Ninth Arbitration Court of Appeal reversed this decision and the reversal was upheld in a cassation ruling by the Court of Intellectual Property Rights, ruling Vkontakte's

---

[210] *Id.* art. 3.

[211] *Id.* art. 7.

[212] *Id.* art. 4.

[213] *Id.* art. 5.

[214] *Id.* art. 6.

[215] *Id.*

[216] *See generally* VKontakte LLC v. Double Data LLC and the National Agency of Credit History, A 40-18827/17, Moscow Arbitration Court 1 (March 22, 2021), https://perma.cc/EF2G-DFDZ.

[217] *Id.* at 2. *See also* Russian Civil Code, art. 1260 (defining "database" as "an aggregate, presented in an objective form, of independent materials (articles, calculations, normative acts, court decisions and other similar materials) which are systematised so that these materials can be found and processed by means of a computer.").

[218] *VKontakte*, A 40-18827/17, Moscow Arbitration Court, at 2.

exclusive right as the database manufacturer has been violated.[219] The decision was grounded on Article 1334 of the Civil Code which provides that the manufacturer of a database has the exclusive right to extract materials from the database and to control their subsequent use in any form and by any means.[220] The defendant companies were banned from collecting further data from Vkontakte profiles and charged a symbolic compensation.[221]

What makes this case interesting is the fact that although the disputed asset was the personal information of the users, the court did not refer to any privacy laws, instead considering the case exclusively in the realm of intellectual property law.[222]

D. Liability

A breach of Russian privacy laws can lead to disciplinary, civil, administrative, and criminal liability. The Russian Civil Code, for example, regulates liability by providing for property damages, moral damages, or lost profits in the case of a violation.[223] The Russian Code of Administrative Violations generally regulates administrative offenses in connection with the processing of personal data or distribution of marketing communications.[224]

On February 7, 2017, Russian President Vladimir Putin signed into law a bill introducing amendments to the Code of Administrative Violations that increased the number of offences from one to seven and increased the maximum fines for certain violations from RUB 10,000 to RUB 75,000 (approximately $170 to $1,260).[225]

The original language of Article 13.11 of the Code of Administrative Violations was very general and broadly regulated violations of the procedure for collecting, keeping, using, or disseminating information about citizens (i.e., personal data).[226] Since July 2017, the Code of Administrative Violations has been further amended to increase the number of fines and diversify the various data protection breaches into specific violations. The below fines are now applicable, unless the offence constitutes a crime, for the following data infringements:[227]

---

[219] *See generally* VKontakte LLC v. Double Data LLC and the National Agency of Credit History, A 40-18827/17, Court of Intellectual Property Rights 2–4 (July 17, 2018), https://perma.cc/SX6R-AVTB.

[220] *Id.* at 32; Russian Civil Code, art. 1334.

[221] *See VKontakte*, A 40-18827/17, Moscow Arbitration Court, at 2. *See generally VKontakte*, A 40-18827/17, Court of Intellectual Property Rights, at 37–40.

[222] *See, e.g.*, *VKontakte*, A 40-18827/17, Court of Intellectual Property Rights, at 12–15.

[223] Russian Civil Code, arts. 15, 151; Federal Law No. 152-FZ, art. 24.

[224] KODEKS ROSSIĬSKOĬ FEDERATSII RF OB ADMINISTRATIVNYKH PRAVONARUSHENIIAKAH [KOAP RF] [Code of Administrative Violations], https://perma.cc/JW5S-B2BR.

[225] Federal'nyĭ Zakon RF No. 405-FZ o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty Rossiĭskoĭ Federatsii [Russian Federal Law No. 405-FZ on the Introduction of Amendments to the Administrative Offenses Code of the Russian Federation], SZ RF 2019.

[226] Russian Code of Administrative Violations, art. 13.11.

[227] Federal'nyĭ Zakon RF No. 405-FZ o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty Rossiĭskoĭ Federatsii [Russian Federal Law No. 405-FZ on the Introduction of Amendments to the Administrative Offenses Code of the Russian Federation], SZ RF 2019, No. 49, Item 6964, art. 1, http://www.consultant.ru/document/cons_doc_LAW_339082/3d0cac60971a511280cbba229d9b6329c07731f7/ (last visited June 26, 2022).

Violation Description	**Fine for Citizens (RUB)**	**Fine for Official (RUB)**	**Fine for Legal Entities (RUB)**
Data processing in cases not provided for by applicable law, as well as data processing incompatible with the purposes of processing	2,000 to 6,000	10,000 to 20,000	60,000 to 100,000
Data processing without written consent, when such consent must be obtained in accordance with the law or if data processing performed with written consent does not meet the mandatory requirements for the composition of information	6,000 to 10,000	20,000 to 40,000	30,000 to 150,000
Failure by the operator to publish or provide access to the privacy policy or information on data protection requirements	1,500 to 3,000	6,000 to 12,000	30,000 to 60,000
Failure by the operator to fulfill the obligation to provide the subject of personal data with information regarding the processing of his personal data	2,000 to 4,000	8,000 to 12,000	40,000 to 80,000
Non-fulfillment (within the established period) of a request for clarification, blocking, or destruction of personal data (in cases where personal data is incomplete or outdated, inaccurately or illegally obtained, or not needed for the stated purpose of data processing)	2,000 to 4,000	8,000 to 20,000	50,000 to 90,000
Non-compliance by the operator in the event of data processing without the use of automatic means of the obligation to comply with conditions ensuring the safety of personal data during the storage of material media and excluding unauthorized access to them, if this led to illegal or accidental access to personal data or their destruction, modification, blocking, copying, presentation of distribution, or other illegal actions	1,500 to 4,000	8,000 to 20,000	50,000 to 100,000
Failure by the operator, which is a state or municipal body, to comply with the statutory obligation to anonymize personal data or non-compliance with the requirements or methods for depersonalization	n/a	n/a	6,000 to 12,000

Failure by the operator to collect personal data, including through the information and telecommunication network "Internet," provided for by the legislation of the Russian Federation in the field of personal data, the obligation to record, organize, accumulate, store, clarify (update, change), or extract personal data of citizens of the Russian Federation using databases located on the territory of the Russian Federation	30,000 to 50,000	100,000 to 200,000	1 million to 6 million
Repeated commission of the above-mentioned offenses	50,000 to 100,000	500,000 to 800,000	6 million to 8 million

Federal Law No. 405-FZ also amended Articles 28.3 and 28.4 of the Code to simplify the process of holding operators liable for personal data law infringements; now Roskomnadzor can unilaterally initiate administrative proceedings without having to involve state prosecutors.[228]

Finally, the Russian Criminal Code contains four main provisions related to data protection: (1) invasion of personal privacy; (2) violation of secrecy of correspondence, telephone conversations, postal, telegraphic, or other messages; (3) refusal by an official to submit information to an individual; and (4) illegal access to computer information.[229] Sanctions for these crimes can reach a fine of up to RUB 200,000 or imprisonment for up to seven years, depending on the crime.[230]

Russian data privacy legislation is in many ways similar to the GDPR, as the above demonstrates that Russia has adopted many European concepts such as the definition of personal data, the right to be forgotten, and key principles of data processing. Increased sanctions in the Russian Administrative and Criminal Codes also show a general awareness of the significance of the right to privacy and its protection. Nevertheless, some overlapping similarities in the regulatory approaches of the Russian and EU data privacy regimes do not give grounds to conclude a harmonization between laws in the two jurisdictions. A deeper analysis of the rights and responsibilities of operators reveals a different approach: The Russian approach, unlike the EU, grants processors the right to determine the goals and means of processing personal data. Additionally, data controllers are not explicitly regulated by Russian law as they are under the GDPR.

The Russian approach to data privacy regulation is also more hands-on than that of the U.S. Russian laws have stricter governmental regulations and do not leave it to the market to resolve issues of privacy through contractual relationships between private actors. This distinction between the Russian and U.S. approach is partly due to differences in common law and civil legal systems as well as variations in

[228] *Id.*

[229] UGOLOVNYĬ KODEKS ROSIĬSKOĬ FEDERATSII [UK RF] [Criminal Code] arts. 137, 138, 140, 272, https://perma.cc/VEG2-V8JV.

[230] *Id.*

governmental organization. It should be noted, however, that certain U.S. states have implemented data privacy regimes that hew more closely to that of the EU and Russia.

V. GLOBAL CROSS-BORDER TRANSMISSION OF PERSONAL DATA

Technological progress has facilitated the free flow of data around the globe and has opened up opportunities for global businesses and human communication. As this trend continues to develop, regulators and governments around the world have become increasingly concerned about data sovereignty.

Under the GDPR, data transfers to other jurisdictions not within the European Economic Area (EEA) or to international organizations is allowed only if such transfers "ensure[] an adequate level of protection."[231] The European Commission sets the following criteria for such adequate protection:

> (a)[T]he rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
>
> (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States;
>
> (c) the international commitments the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."[232]

The European Commission publishes a list of countries and international organizations where such standards of adequate protection have been met.[233]

A controller (a person or entity that determines the purposes and means of processing personal data) or a processor (a person or entity that processes data on

---

[231] General Data Protection Regulation, *supra* note 1, arts. 44–50.

[232] *Id.* art. 45.

[233] *Adequacy Decisions*, EUR. COMM'N, https://perma.cc/HD3C-TDEL.

behalf of the controller) must ensure appropriate safeguards in cross-border data transfers. One option for doing so is getting the consent of the party whose data is being transferred. Other options include the use of Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs). SCCs can be used to govern transfers between controllers, as well as transfers between a controller (as the exporter) and a processor (as the importer).

Similar to the GDPR, Russia's privacy laws permit cross-border transmission of personal data to territories that provide "adequate protection" of personal data. Cross-border transmission of personal data is defined by Russian Federal Law No. 152-FZ as the "transfer of personal data to a foreign state agency, foreign legal entity or individual located in a foreign state."[234] Article 12 of the law specifies that transmission can be made to states that are parties to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, as well as other countries that provide "adequate protection."[235]

Specifically, Article 12 provides that prior to commencing the cross-border transmission of personal data, operators must make sure that the foreign state to which the personal data are to be transmitted provides adequate protection of the rights of personal data subjects, with adequate protection defined in terms of foreign states having legal rules conforming to the same standards as the Convention.[236] Any cross-border transmission of personal data—even to foreign states providing adequate protection—must be performed in accordance with the other provisions of Federal Law No. 152-FZ, and even then transfers "may be prohibited or restricted for the purposes of protecting the foundations of the constitutional order of the Russian Federation, public morality and health, rights and legitimate interests of citizens and providing for national defense and state security."[237] The cross-border transmission of personal data to the territory of foreign states that do not provide adequate protection of the rights of personal data subjects may still be performed in several instances, such as:

1. The consent of the personal data subject;
2. Under federal law it is necessary to protect the fundamental principles of the constitutional order or to ensure the national defense and security of the state;
3. Performance of a contract the personal data subject is a party to; or
4. Protection of the life, health, or other vital interests of the personal data subject or other persons, and it is impossible to obtain the personal data subject's consent.[238]

Like the European Commission, Roskomnadzor maintains a list of foreign states that are not members of the Convention but still provide "adequate protection."[239]

---

[234] Russian Federal Law No. 152-FZ, art. 3(11).

[235] *Id.* art. 12.

[236] *Id.*

[237] *Id.*

[238] *Id.*

[239] Prikaz Roskomnadzora ot 15.03.2013 No. 274 (red. ot 14.09.2021) ob Utverzhdenii Perechnia Inostrannykh Gosudarstv, Ne Iavliaiushchikhsia Storonami Konventsii Soveta Evropy o Zashchite Fizicheskikh Lits Pri Avtomatizirovannoĭ Obrabotke Personal'nykh Dannykh I Obespechivaiushchikh

Localization requirements of personal data under Russian law become complicated in the case of cross-border transmission, which leads to localization of data on foreign servers. This problem was solved by Roskomnadzor instituting a division of all databases into primary and secondary databases.[240] Primary databases must be located in Russia and secondary copies can be located in foreign jurisdictions.[241] However, this localization requirement applies only to situations in which personal data is collected directly from data subjects.[242]

On November 17, 2016, Roskomnadzor blocked access to LinkedIn within Russia for violations of Russia's Federal Law No. 149-FZ, which, among other things, requires that data operators store the personal data of Russian citizens on servers located within Russia's borders.[243]

On January 31, 2020, Roskomnadzor initiated administrative cases against Facebook and Twitter for refusing to provide details on data localization for Russian users in accordance with Federal Law No. 152-FZ and other Russian regulations.[244] On February 13th, the Tagansky District Court of Moscow fined Facebook and Twitter for RUB 4 million each.[245] Both companies were found guilty of violating Part 8 of Article 13.11 of the Code of Administrative Violations which penalizes failures by the operator to fulfill the obligation to store personal data of Russian citizens in the country.[246] It is expected that Russia will carry out similar enforcement actions against other non-Russian companies that it finds to be non-compliant with Russian data protection and privacy regulations.

More detailed mechanisms of transborder flow of personal data between Russia and other jurisdictions are regulated by the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[247] Article 17 of the Protocol amends Article 12 of the Convention stipulating that parties to the Convention:

Adekvatnuiu Zashchitu Prav Sub"ektov Personal'nykh Dannykh [Roskomnadzor Order No. 274 of March 15, 2013 (as amended on September 14, 2021) on Approval of the List of Foreign States That Are Not Parties to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data and Ensure Adequate Protection of the Rights of Personal Data Subjects], http://www.consultant.ru/document/cons_doc_LAW_145512/.

[240] *See Russia's Personal Data Localization Law Goes into Effect*, DUANE MORRIS: ALERTS AND UPDATES (Oct. 16, 2015), https://perma.cc/VUP3-6EWA.

[241] *Id.*

[242] Federal'nyĭ Zakon RF No. 242-FZ [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], SZ RF 2014, No. 242, art. 2, https://perma.cc/UA3E-U5N6; Federal'nyĭ Zakon RF No. 152-FZ o Personal'nykh Dannykh [Federal Law of the Russian Federation on Personal Data], SZ RF 2006, No. 31, Item 3451, art. 18(5), https://perma.cc/MXC3-4RU4.

[243] Adam Taylor, *Russia Moves to Block Professional Networking Site LinkedIn*, WASH. POST, Nov. 17, 2016; Russian Federal Law No. 149-FZ, art. 16(4)(7).

[244] Sergei Blagov, *Facebook, Twitter Fined in Russia Over Data-Storage Practices*, BLOOMBERG LAW, Feb. 13, 2020; Russian Federal Law No. 152-FZ, art. 22(3)(10.1).

[245] *Twitter, Facebook Fined for Not Moving User Data to Russia*, AP NEWS (Feb. 13, 2020), https://perma.cc/HU29-Y3M7.

[246] Russian Code of Administrative Violations, art. 13.11.

[247] Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Oct. 10, 2018, C.E.T.S. No. 223.

> [S]hall not prohibit or subject to special authorisation the transfer of data to a recipient who is subject to the jurisdiction of another Party to the Convention. Such a Party may, however, do so if there is a real and serious risk that the transfer to another Party, or from that other Party to a non-Party, would lead to circumventing the provisions of the Convention. A Party may also do so if bound by harmonised rules of protection shared by States belonging to a regional international organization.[248]

However,

> [E]ach Party may provide that the transfer of personal data may take place if the data subject has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards or the specific interests of the data subject require it in the particular case; or prevailing legitimate interests, in particular important public interests, are provided for by law and such transfer constitutes a necessary and proportionate measure in a democratic society; or it constitutes a necessary and proportionate measure in a democratic society for freedom of expression.
>
> Each Party shall provide that the competent supervisory authority . . . is provided with all relevant information concerning the transfers of data . . . and that the supervisory authority is entitled to request that the person who transfers data demonstrates the effectiveness of the safeguards or the existence of prevailing legitimate interests and that the supervisory authority may, in order to protect the rights and fundamental freedoms of data subjects, prohibit such transfers, suspend them or subject them to conditions.[249]

The U.S. does not place any restrictions on the transfer of personal data to private entities in other jurisdictions. However, businesses established in other jurisdictions are subject to federal data protection laws for data concerning U.S. residents, as well as to relevant state laws based on the state of residence of any individual whose information the business collects, holds, transmits, processes, or shares. Practically, however, U.S. companies cannot conduct business with entities or individuals in the EEA in particular without ensuring adequate data protection safeguards under GDPR standards. The European Commission has approved a few countries as generally assuring adequate data protection levels, including Argentina, Canada, Israel, New Zealand, Switzerland, and Uruguay, but has gone back and forth on an adequacy finding for the U.S.[250]

The International Trade Administration (ITA) within the U.S. Department of Commerce established EU-U.S. and Swiss-U.S. Privacy Shield Frameworks,

---

[248] *Id.* art. 17, ¶ 2.

[249] *Id.* art. 17, ¶¶ 4(a)–(d), 6.

[250] *Adequacy decisions*, European Commission, https://perma.cc/S9AV-ANKX. *See also* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. *(Schrems II)*, ECLI:EU:C:2020:559 (July 16, 2020) (invalidating the Privacy Shield framework); Case C-362/14, Schrems v. Data Prot. Comm'r *(Schrems I)*, ECLI:EU:C:2015:650 (Oct. 6, 2015) (invalidating the Safe Harbor framework). *But see* Press Release, *European Commission and United States Join Statement on Trans-Atlantic Data Privacy Framework*, EUR. COMM'N (Mar. 25, 2022), https://perma.cc/VW6Q-ZTX7.

which were designed to provide a compliance mechanism for transferring personal data from the EU and Switzerland to the U.S.[251] On July 12, 2016, the European Commission Parliament validated the adequacy of the EU-U.S. Privacy Shield as a legal mechanism to enable data transfers under EU law.[252] On passage of the GDPR, the European Commission also validated a set of standard commercial clauses (SCCs) that provided a safeguard for the international transfer of personal data to the U.S. if not modified (except to include additional business-related clauses).[253]

In July 2020, however, the Court of Justice of the European Union (ECJ) invalidated the EU-U.S. Privacy Shield in a decision known as *Schrems II*.[254] In *Schrems II,* the ECJ concluded that certain U.S. laws which regulate government authorities' access and use of personal data imported from the EU into the U.S. created the risk that EU citizens whose data was accessed in the course of U.S. national security investigations might not be afforded the protections required under the GDPR.[255] In June 2021, the European Commission implemented new SCCs that provide appropriate safeguards regarding personal data transfers out of the EU to third countries not recognized as ensuring an adequate level of protection, as well as another set of SCCs made as part of data processing agreements (DPAs) between controllers and processors.[256]

---

[251] *See* U.S. DEP'T OF COM., EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES 2 (2016), https://perma.cc/C4RA-LFHG.

[252] Commission Implementing Decision 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and the Council, 2016 O.J. (L 207); *Swiss-US Privacy Shield: New Legal Framework for the Transfer of Data to the USA*, SWITZ. FED. DATA PROT. AND INFO. COMM'R (Jan. 11, 2017) https://perma.cc/YK76-JJKV.

[253] General Data Protection Regulation, *supra* note 1, art. 28(8) (enabling EU supervisory authorities to adopt standard contractual clauses for DPAs). *See Sous-traitance: Exemple de clauses* [*Subcontracting: Examples of Clauses*] CNIL (Oct. 4, 2017), https://perma.cc/YU3Z-QG7K; *Directrices para la elaboración de contratos entre responsables y encargados de tratamiento* [*Guidelines for the preparation of contracts between controllers and processors*], AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, https://perma.cc/C42H-3KVN. Denmark, Slovenia and Lithuania have also submitted to the European Data Protection Board (EDPB) draft standard contractual clauses for DPAs under GDPR Article 28. *See DK SA Standard Contractual Clauses for the purposes of compliance with art. 28 GDPR (January 2020)*, EUR. DATA PROT. BD. (Jan. 1, 2020), https://perma.cc/9K3X-GGFV; *Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the SI SA (Article 18(8) GDPR)*, EUR. DATA PROT. BD. (May 19, 2020), https://perma.cc/46A8-D5XU; *Opinion 18/2021 on the draft Standard Contractual Clauses submitted by the LT SA (Article 28(8) GDPR)*, EUR. DATA PROT. BD. (May 19, 2021), https://perma.cc/EN45-PTUR.

[254] Case C-311/18, Data Prot. Comm'r v. Facebook Ir. & Maximillian Schrems (Schrems II), ECLI:EU:C:2020:559, (July 16, 2020).

[255] *Id.* at **43–45 (referencing 50 U.S. C. §1881, U.S. Foreign Intelligence Surveillance Act (FISA) Amendments of 2008, § 702 (2012); Exec. Order No. 12333, 3 C.F.R. § 200 (1981); and Presidential Policy Directive 28 Signals Intelligence Activities (Jan. 17, 2014)).

[256] Commission Implementing Decision 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation 2018/1725 of the European Parliament and of the Council, 2021 O.J. (L199) 18; Commission Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation 2016/679 of the European Parliament and of the Council, 2021 O.J. (L 199) 31; *see also* General Data Protection Regulation, *supra* note 1, arts. 46(1)–(2)(c), 28(7) (governing new SCCs and SCCs for DPAs respectively).

VI. INTERNATIONAL TREATIES

In addition to the constitutional rights and legislation noted above, international treaties form a critical component of global data privacy law. The U.S. and the EU (but not Russia), for example, are parties to the Convention on Cybercrime (also called the Budapest Convention).[257] The Budapest Convention requires the sixty-six ratifiers to retain the authority to compel companies within their territory to disclose stored electronic data subject to their jurisdiction. [258]

The Budapest Convention places territorial limits on this compulsory power, providing for transborder data access (without the permission of the country where the data is located) in only two instances: (1) the information sought is open-source data, or (2) with the lawful, voluntary consent of the person who has lawful authority to disclose the data.[259]

Absent either of these instances, member parties must go through Mutual Legal Assistance Treaties (MLATs), which enable law enforcement agencies in one country to seek the assistance of foreign counterparts who can legally obtain the sought-after data. The U.S. has several MLATs in place concerning data, including an MLAT with the EU (in place since 2003), which ensures that the states may limit their obligations to provide assistance, that limitations are in place regarding the use of the evidence or information obtained, and that states may be asked to keep the request for information confidential if desired by the requesting state.[260] The U.S. also has an MLAT with Russia concerning criminal matters (including locating and providing assets, documents, records, and other items relevant to, among other things, aggravated identity theft).[261] Unfortunately, MLATs can be complex and time-consuming.[262] Individual countries' law enforcement agencies often have their own legal standards for production of data, and U.S. companies subject to such requests may challenge them in local courts. In addition, MLATs are not consistently adhered to by the U.S. and foreign signatories.[263]

In March 2018, the U.S. enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which amends the Stored Communications Act,[264] by adding the following provision:

---

[257] *Chart of signatures and ratifications of Treaty 185*, COUNCIL OF EUR., https://perma.cc/AHP6-7S7C.

[258] Convention on Cybercrime, art. 18(1), *opened for signature* Nov. 23, 2001, E.T.S. No. 185, *available at* https://perma.cc/3634-X8CQ [hereinafter Budapest Convention]; *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUR., https://perma.cc/F3BH-LESX.

[259] *Id.* art. 32(a)–(b).

[260] Agreement on Mutual Legal Assistance between the United States of America and the European Union, EU-U.S., arts. 9–10, June 25, 2003, T.I.A.S. No. 109-13.

[261] Treaty on Mutual Legal Assistance in Criminal Matters, Russ.-U.S., Feb. 10, 2000, S. TREATY DOC NO. 106–22.

[262] RICHARD CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 227 (2013) ("Requests appear to average approximately 10 months to fulfill, with some requests taking considerably longer.").

[263] ALAN MCQUINN & DANIEL CASTRO, HOW LAW ENFORCEMENT SHOULD ACCESS DATA ACROSS BORDERS 8 (2017), https://perma.cc/8ZDL-P34L.

[264] 18 U.S.C. §§ 2701–13.

> 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.[265]

The CLOUD Act has two distinct parts. As noted above, the CLOUD Act explicitly compels U.S. companies to produce electronic data they possess or control regardless of where it is stored. The CLOUD Act also authorizes the United States to enter into international treaties with other countries to streamline the process for production of electronic data in criminal proceedings. According to the Department of Justice, this part of the CLOUD Act ensures that "[f]or investigations of serious crime, CLOUD agreements can be used to remove restrictions under each country's laws so that Cloud Service Providers (CSPs) can comply with qualifying, lawful orders for electronic data issued by the other country to address conflicts of law."[266] To date, the U.S. has signed one bilateral data-sharing agreement under the CLOUD Act with the United Kingdom[267] and is in negotiations to enter into a bilateral agreement with Australia as well.[268] By contrast, efforts to enter into a bilateral CLOUD Act agreement with the EU have stalled.[269]

In accordance with the provisions of the International Covenant on Civil and Political Rights (ICCPR)[270]—to which the United States, Russia, and EU nations are parties—everyone has the right to freedom of thought[271] and the right to freedom of opinion and expression.[272] The latter right includes freedom to adhere freely to one's beliefs and freedom to seek, receive, and disseminate information and ideas by any means and regardless of state borders.[273] UN Human Rights Committee General Comment No. 34, interpreting the rights enshrined in Article 19, further defines freedom of opinion and expression as "all forms of expression and methods of disseminating opinions, including all types of audiovisual, electronic and Internet-based means of expression."[274]

The European Convention on Human Rights (ECHR)—ratified by forty-seven countries including originally Russia in 1998—guarantees the right to respect

---

[265] Consolidated Appropriations Act of 2018, scc. 103(a)(1), Pub. L. No. 115-141, 132 Stat. 348, 1214 (Mar. 23, 2018) (codified at 18 U.S.C. § 2713) [hereinafter CLOUD Act].

[266] U.S. DEP'T OF JUST., PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 3 (2019), https://perma.cc/D2A4-NBUQ.

[267] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, UK-U.S., Oct. 3, 2019, 60 Int'l Legal Materials 168 (2021).

[268] Press Release, *Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton*, U.S. DEPARTMENT OF JUSTICE (Oct. 7, 2019), https://perma.cc/DS6P-3VPZ.

[269] Theodore Christakis & Fabien Terpan, *EU-US Negotiations on Law Enforcement Access to Data: Divergences, Challenges and EU Law Procedures and Options*, 11 INT'L DATA PRIV. LAW 81, 81–82 (2021).

[270] International Covenant on Civil and Political Rights, Dec. 16, 1966, T.I.A.S. No. 92-908.

[271] *Id.* art. 18.

[272] *Id.* art. 19.

[273] *Id.*

[274] Human Rights Committee General Comment No. 34 (Sept. 12, 2011).

for one's private life in Article 8, freedom of thought in Article 9, and freedom of expression in Article 10.[275] On March 15, 2022, Russia's Ministry of Foreign Affairs informed the Council of Europe of its decision to leave this organization.[276] Based on Article 58 of the ECHR, a party to the treaty may denounce the ECHR after five years from the date on which it became a party to it and after six months' notice addressed to the Secretary General of the Council of Europe.[277] Based on paragraph 3 of Article 58 of the ECHR, the denunciating State ceases to be a party to the ECHR after denunciation.[278] However, Russian domestic law still requires enactment of a specific federal law affirming denunciation of a former treaty ratification in order for the withdrawal to have domestic legal effect.[279] New legislation in this area should be expected in the near term.

Among other relevant international treaties to which Russia is a party, two are important to note in the context of data privacy regulation: (1) the Strasbourg Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ratified by Russia in 2006) and (2) the Protocol Amending the Convention of 2018 (whose purpose is to modernize and improve the Convention, taking into account the new tasks for the protection of individuals in the processing of personal data that arose after the adoption of the Convention in 1980).[280] The modernization of the Strasbourg Convention, the only globally significant binding international treaty in this area, arose from the desire to ensure its effective application to novel data privacy issues raised by "new information and communication technologies."[281] Thus, the Protocol provides a reliable and flexible multilateral legal framework to facilitate cross-border data exchange, while providing effective guarantees for the use of personal data. It constitutes a bridge between different regions of the world and various regulatory frameworks, including the GDPR, which refers to the Convention regarding transboundary data flows.[282]

The Russian Constitution has been amended such that the provisions of the Constitution are prioritized over all international agreements.[283] In other words, the

---

[275] European Convention for the Protection of Human Rights and Fundamental Freedoms, arts. 8–10, April 11, 1950, 213 U.N.T.S. 221 [hereinafter ECHR]; *Chart of signatures and ratifications of Treaty 005*, COUNCIL OF EUR., https://perma.cc/6YPG-XKH8 (last visited May 6, 2022).

[276] *See* Press Release, *Russia Set to Leave Council of Europe and Denounce European Convention on Human Rights*, EUROPEAN HUMAN RIGHTS ADVOCACY CENTRE (Mar. 16, 2022), https://perma.cc/D4DC-J5RN.

[277] ECHR, supra note 275, art. 58.

[278] *Id.*

[279] Federal'nyĭ Zakon RF No. 101-FZ o Mezhdunarodnykh Dogovorakh Rosiĭskoĭ Federatsii [Russian Federal Law No. 101-FZ on International Agreements of the Russian Federation], SZ RF 1995, No. 29, Item 2757,
https://perma.cc/27CW-ADFJ.

[280] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *opened for signature* Jan. 28, 1981, E.T.S. No. 128; Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *opened for signature* Oct. 10, 2018, C.E.T.S. No. 223.

[281] *Modernisation of the Data Protection "Convention 108"*, COUNCIL OF EUR., https://perma.cc/QAF6-NXWM.

[282] General Data Protection Regulation, *supra* note 1, Recital 105.

[283] Federal'nyĭ Zakon RF No. 7-FKZ o Vnesenii Izmeneniĭ v Federal'nyĭ Konstitutsionnyĭ Zakon o Konstitutsionnom Sude Rosiĭskoĭ Federatsii [Russian Federal Law No. 7-FKZ on Amendments to the Federal Constitutional Law on the Constitutional Court of the Russian Federation], SZ RF 2015, No. 51, Item 7229, https://docs.cntd.ru/document/420322320.

amendments authorized the Russian Constitutional Court to give the Russian Constitution priority and decline to follow international treaties or agreements that are inconsistent with the Russian Constitution. As a result of these amendments, we will see multiple changes in the Russian approach to international agreements in the future.

VII. CONCLUSION

Globalization invites a singular regulatory approach to data protection, especially in cases of cross-border transmission. However, cultural, national, and commercial norms related to issues like data localization, restrictions on privacy for public safety purposes, and technological innovation continue to drive unique, country-specific (and regional) approaches. To date, the GDPR is the dominant global standard. It views protection of personal data as a basic human right (irrelevant of nationality) and has an extraterritorial reach that extends to any data subject whose personal data is processed (or controlled) in the EU.[284] Compliance with these and other GDPR requirements have presented significant complications for non-EU countries and companies.

For example, while the Russian data privacy law and the GDPR are similar in their approach, GDPR compliance presents challenging issues for Russian companies in practice. Unlike the GDPR, the Russian Federal Law No. 242-FZ does not have an extraterritorial effect and thus does not apply to non-residents collecting personal data of Russian citizens abroad (unless they operate on the Internet directed to the Russian Federation).[285] However, Russia places a stronger emphasis on data localization requirements for primary databases containing personal information of Russian citizens, which must be located on Russian servers.[286] Under the GDPR, the server location doesn't matter as much as the location where the decisions concerning the data processing are taken.[287] On top of navigating these differences, Russian companies still need to identify how to operationalize the GDPR's technical and document reporting requirements.

The divergent approaches to data privacy in the U.S. on the one hand and in Russia the EU on the other can perhaps best be described as the U.S. asking *why* data is being collected, while Russia and the EU focus on *whose* data is being collected. This fundamental difference has left U.S. companies struggling to comply with the GDPR in a way that does not also conflict with U.S. laws and regulations.[288] This tension, coupled with the cost and burden of GDPR compliance, has led many mid-

---

[284] *See supra* Part II.A.

[285] *See* Federal'nyĭ Zakon RF No. 242-FZ o Vnesenii Izmeneniĭ v Otdel'nye Zakonodatel'nye Akty Rossiĭskoĭ Federatsii v Chasti Utochneniia Poriadka Obrabotki Personal'nykh Dannykh v Informatsionno-Telekommunikatsionnykh Setiakh, [Amending Some Legislative Acts of the Russian Federation as It Concerns Updating the Procedure for Personal Data Processing in Information Telecommunication Networks], SZ RF 2014, No. 30, Item 4243, art. 2, https://pd.rkn.gov.ru/authority/p146/p191/ (requiring operators provide for the collection of personal data for databases located within the Russian Federation for the retrieval of the personal data of Russian citizens); *supra* Part IV.B.

[286] *See supra* Part V.

[287] *See supra* Part II.

[288] *See Potential Conflict and Harmony between GDPR and the CLOUD Act*, REED SMITH: CLIENT ALERTS (June 14, 2018), https://perma.cc/TE7X-FR4C (analyzing the potential for companies to have conflicting obligations between the GDPR and CLOUD Act).

sized and small U.S.-based companies to cease operations in Europe.[289] At the same time, it has also led to major U.S. tech companies—who are often in the best position to bear the expense and burden of complying with the GDPR—facing the largest fines for GDPR non-compliance.[290]

The myriad of conflicting laws and federal regulations only exacerbates the issue. The impact of California's recently enacted GDPR-like CPRA is beginning to be felt, and calls for federal privacy legislation in the U.S. are growing.[291] Several comprehensive data privacy bills are pending in the U.S. Congress, and many of the U.S.'s largest technology companies have joined the call for legislation that will bring a uniform, federal approach to data privacy that preempts emerging state data privacy laws.[292] Following the *Schrems II* decision, it is even more imperative that the U.S. adopt federal privacy standards that would align U.S. practices with those of its allies and trading partners.

---

[289] *See, e.g.*, Hannah Kuchler, *US Small Businesses Drop EU Customers Over New Data Rule*, FIN. TIMES (May 23, 2018), https://perma.cc/Q928-BGX7 ("[S]ome smaller US companies believe the potential risks outweigh the benefits of operating in the EU, particularly if they have to make expensive changes to their products and services to comply."); Edward Longe, *GDPR Was Bad for Europe; U.S. Needs Its Own Path*, INSIDE SOURCES (Dec. 8, 2021), https://perma.cc/QP7M-GVV3 ("The onerous provisions of GDPR have also forced many American companies to abandon or reduce services in Europe, deeming compliance more expensive.").

[290] *See supra* Part II.C.

[291] *See supra* Part III.B.

[292] *Id.*