2023

Who Owns Data? Constitutional Division in Cyberspace

Dongsheng Zang

Who Owns Data? Constitutional Division in Cyberspace

Dongsheng Zang

AUTHOR'S NOTE:

Associate Professor of Law, University of Washington School of Law. I would like to thank Xuan-Thao Nguyen, Jennifer S. Fan, and Norman Page. My colleagues at the Gallagher Law Library provided me with superb assistance in locating information and materials. I wish to thank Ms. Cindy Fester for her capable editorial assistance in the early stage of the manuscript. I wish to thank Kabi N. Palaniappan and Kathryn A. Quelle of the Journal of Transnational Law & Contemporary Problems for their excellent assistance in shaping and improving the manuscript. Of course, all errors are mine.

I. INTRODUCTION

Privacy emerged as a concern as soon as the internet became commercial. In early 1995,[1] Lawrence Lessig warned that the internet, though giving us extraordinary potential, was "not designed to protect individuals against this extraordinary potential for others to abuse."[2] The same technology can "destroy the very essence of what now defines individuality."[3] Lessig urged that "a constitutional balance will have to be drawn between these increasingly important interests in privacy, and the competing interest in collective security."[4] Lessig envisioned that creating property rights in data would help individuals by giving them control of their data.[5] As utopian as property rights in data seemed, it was a shared vision before September 11, 2001 (hereinafter September 11).[6] For convenience, I will call this school of thought the "data subject's property" (DSP) theory of data. DSP builds on the foundation of *Katz v. United States*, where the United States Supreme Court declared that the Fourth Amendment "protects people, not places."[7]

After September 11, Congress passed the USA Patriot Act.[8] The government launched massive surveillance programs in secret.[9] Policing

---

[1] Two significant events happened in the year 1995 in the history of the internet: the first was Netscape's successful IPO on August 9, 1995, and the second was Bill Gates' May 26, 1995 memo "The Internet Tidal Wave," which laid out Microsoft's strategy for the internet era. Windows 95 was rolled out in August 1995. *See* SHANE M. GREENSTEIN, HOW THE INTERNET BECAME COMMERCIAL: INNOVATION, PRIVATIZATION, AND THE BIRTH OF A NEW NETWORK 159–86 (Princeton Univ. Press 2015).

[2] Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1749 (1995).

[3] *Id.* at 1748.

[4] *Id.* at 1752.

[5] [A] property regime requires negotiation before taking; a liability regime allows a taking, and payment later. The key to a property regime is to give control, and power, to the person holding the property right; the key in a liability regime is to protect the right but facilitate the transfer of some asset from one person to another." "Property protects choice; liability protects transfer." LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160–61 (1999).

[6] Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996); J.H. Reichman & Pamela Samuelson, *Intellectual Property Rights in Data*, 50 VAND. L. REV. 49 (1997); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998); James Rule & Lawrence Hunter, *Towards Property Rights in Personal Data*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 168–81 (Colin J. Bennett & Rebecca Grant eds., 1999); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

[7] Katz v. United States, 389 U.S. 347, 351 (1967).

[8] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[9] Surveillance programs remained secret until they were revealed by Edward Snowden in 2013. *See* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014); BARTON GELLMAN, DARK MIRROR: EDWARD SNOWDEN AND THE AMERICAN SURVEILLANCE STATE (Penguin Publ'g. Grp. 2020); *see also* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

shifted towards intelligence gathering.[10] Jack M. Balkin, a leading constitutional law scholar, argued that the United States has gradually transformed into a "National Surveillance State," meaning a new form of governance that "features the collection, collation, and analysis of information about populations both in the United States and around the world."[11] Balkin issued his warnings in the midst of mounting demands for the DSP—property protection of personal data.[12] Like those urged by Lessig ten years earlier, demands for DSP in the aftermath of September 11 were timely in terms of technological development: this was the time that Web 2.0 (e.g., social media) was emerging.[13] According to Shoshana Zuboff, a retired professor from Harvard Business School, 2002 was a "watershed year during which surveillance capitalism took root."[14] It was in August 2002 that Google shifted its business model towards targeted advertisement. Mark Zuckerberg founded Facebook in his Harvard dorm, beginning the new era of social media in January 2002.[15] If DSP had been better embraced and better policies adopted, then privacy would have been better protected.

This Article does not attempt to make an additional argument following the normative line of DSP. Rather, it asks what happened to the DSP theory of data and why has it been sidelined? For this purpose, this Article proposes to examine privacy in cyberspace by tracking the competition between DSP and its rival theories in defining privacy. Samuel Warren and Louis Brandeis initially proposed that privacy be a *personal* right,[16] much like DSP; however,

---

[10] Andrew Guthrie Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 EMORY L.J. 259 (2012); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015); Barry Friedman & Cynthia Benin Stein, *Redefining What's "Reasonable": The Protections for Policing*, 84 GEO. WASH. L. REV. 281 (2016); BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION (2017).

[11] Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3 (2008) ("The National Surveillance State grows naturally out of the Welfare State and the National Security State; it is their logical successor.") [hereinafter Balkin, *Surveillance State*]. *See also* Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006).

[12] James B. Rule, *Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions*, 54 U. TORONTO L.J. 183 (2004); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2004); Margaret Jane Radin, *Incomplete Commodification in the Computerized World*, in THE COMMODIFICATION OF INFORMATION 3 (Niva Elkin-Koren & Neil Weinstock Netanel eds., 2002); Margaret Jane Radin, *A Comment on Information Propertization and Its Legal Milieu*, 54 CLEV. ST. L. REV. 23 (2006); Barbara J. Evans, *Much Ado about Data Ownership*, 25 HARV. J. L. & TECH. 69 (2011).

[13] Tim O'Reilly, "What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software" (Sept. 30, 2005), available at: https://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html (last visited, Oct. 30, 2022); also, PAUL ANDERSON, WEB 2.0 AND BEYOND: PRINCIPLES AND TECHNOLOGIES (2012).

[14] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN NATURE AT THE NEW FRONTIER OF POWER 75 (2019).

[15] ROGER MCNAMEE, ZUCKED: WAKING UP TO THE FACEBOOK CATASTROPHE 53–54 (2019).

[16] *Infra,* text accompanying notes 39 and 43.

Olmstead v. United States shifted this view, finding the right of privacy attached to a defendant's property, not to her person.[17] This decision was the product of an era of government expansion, when the police, tax bureau, or liquor agency were the data collectors. The second shift came when the Warren Court ruled in *Katz* that privacy was personal, not based on property; however, the Burger Court soon created the third-party doctrine, [18] under which voluntarily submitting information to a third-party, such as a telephone company or bank, defeats the privacy right.[19] The third-party doctrine is a claim that data are the property of the collector. The third shift developed in the era of the internet and social media; despite the warnings of Lessig and Balkin, as well as occasional protests from tech companies, the Roberts Court brought the third-party doctrine to cyberspace through *Jones* and *Carpenter*.[20] This time the data collectors are familiar digital platforms. Therefore, throughout the history of privacy, the DSP was met with a rival theory called "data collector's property" (DCP) theory. The DSP-DCP competition is a powerful thread in revealing the internal logic of a surveillance state in the United States where data collectors—whether they be government agencies, private companies, or digital platforms—have dominated and defined privacy.

Undoubtedly, the history of DCP domination is a history of how the Supreme Court impoverished the Fourth Amendment, and such impoverishment is further entrenched in cyberspace. Informative as it is, however, the DSP-DCP competition in one country is not enough to enable us to assess the level and characteristics of such impoverishment. For that purpose, two comparative perspectives are needed. One such perspective is the European Union's experience, where the notion of privacy based on "personality rights" is rooted in the Civil Law tradition and is closer to the DSP theory. [21] This legal analysis allows the EU courts to more often find constitutional principles applicable, thus the judiciary is enabled to elaborate on constitutional norms and prescribe rules for the legislature to follow. By contrast, in the United States, courts often focus their legal analysis on attributes of the particular technology, and their legal reasoning is characterized by piecemeal and binary judgments. In other words, a comparison with the EU experience reveals that the DCP domination in the United States means the federal courts have long ceased to be a constitutional court.

---

[17] Olmstead v. United States, 277 U.S. 438 (1928). For discussion of the case, *infra*, text accompanying notes 68 and 74.

[18] *Infra*, text accompanying notes 89 and 110.

[19] United States v. New York Tel. Co., 434 U.S. 159 (1977), for discussion, *infra*, text accompanying notes 106 and 107. United States v. Miller, 425 U.S. 435 (1976), for discussion, *infra*, text accompanying notes 94 and 97.

[20] United States v. Jones, 565 U.S. 400 (2012), for discussion, *infra*, text accompanying notes 114 and 124. United States v. Carpenter, 138 S.Ct. 2206 (2018), for discussion, *infra*, text accompanying notes 125 and 142.

[21] *Infra,* Part III.

The other comparative perspective is privacy in illiberal states. A brief survey of Turkey, Russia, and China shows that privacy in illiberal societies is also dominated by DCP theory—the difference is that the surveillance state itself is increasingly becoming the data collector. This is driven by the need for illiberal societies to exercise direct control over data, including censorship, suppression, and complete domination. Thus, comparison with illiberal states enables us to see in the United States a surveillance state embedded in surveillance capitalism. It is a mutually dependent, symbiotic relationship. This is accomplished by a diluted Fourth Amendment that balances the mutual relationship and benefits both sides. In terms of ideology, however, the surveillance state in the United States and those in illiberal states do have something fundamental in common: they both insist data is the property of data collectors, not the data subjects.

II. THIRD-PARTY'S PROPERTY: THE UNITED STATES

In the United States, the DCP-DSP competition evolved around the technology and the entities involved in data collection. In the era of the internet and social media, the most obvious data collectors are the digital platforms like Google and Facebook. Another category of data collectors are law enforcement and other government agencies. Despite the DSP demands, DCP theories prevailed in courtrooms, most notably through the Roberts Court's rulings in *United States v. Jones*,[22] and *Carpenter v. United States*,[23] as well as federal circuit courts in "private search" doctrine cases. The goal of this Part is to demonstrate how DCP theories, in various forms, have dominated the interpretation of the Fourth Amendment in the era of Web 2.0. However, these DCP theories are not new; they have been established in the earlier eras in competition with earlier DSP claims. For that reason, discussion in this Part follows a chronological order.

Section A provides the historical background of privacy, from the Warren and Brandeis article to *Olmstead*, to *Katz*, and then to *United States v. Miller*. It aims to make the case that prior to the arrival of the internet, DCP theories have secured their domination in the competition with DSP. After this historical and doctrinal background, subsequent sections explain how the earlier DCP theories were brought to cyberspace. Section B explains how *Jones* revitalized *Olmstead*; Section C how *Carpenter* revitalized *Miller*; Section D explains how the "private search" doctrine was brought to the cloud. The Roberts Court has not spoken on this doctrine in the context of cyberspace, but federal circuit courts seem have reached enough consensus. The aim of Sections B, C and D is to demonstrate how the Fourth Amendment is dominated by DCP theories despite repeated callings of DSP.

[22] United States v. Jones, 565 U.S. 400 (2012).

[23] Carpenter v. United States, 138 S.Ct. 2206 (2018).

A. How Property Defined Privacy

Prior to the internet and social media, there were two major rounds of DSP-DCP struggle. The first DSP offensive occurred in 1890, when Samuel Warren and Louis Brandeis published their celebrated article on privacy.[24] It was an era of photography and telegraphy, in addition to the existing commercial press. The call for a new concept of privacy was based on the claim that traditional tort law inadequately protected certain individual interests.[25] However, the Supreme Court's ruling in the wiretapping case *Olmstead* forcefully directed the debate to the notion of property.[26] *Olmstead* started a new era in which the telephone was the main technology, while the government increasingly became the data collector. The second DSP offensive started magnificently with *Katz*, in which the Warren Court famously announced that the Fourth Amendment "protects people, not places."[27] However, the Burger Court came up with an innovative DCP theory called the "third-party doctrine" in *United States v. Miller*,[28] and *Smith v. Maryland*.[29] The doctrine, developed in the era of telephone, computers, and government agencies as data collectors, established the foundation for the internet era.

1. Privacy as Personal Rights

At its creation, the notion "to be let alone"[30] for Judge Thomas M. Cooley seemed a component of the broader category of "personal rights."[31] He argued that damage in such a case was not merely pecuniary loss or pain,[32] but rather, "the personal affront and indignity which are given by the wrongful act."[33] Furthermore, Judge Cooley distinguished this new type of tort from defamation libel. While in libel, truthfulness was a complete defense, "here the very truthfulness of the charge may render it . . . injurious."[34] Judge Cooley

---

[24] Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[25] *Infra,* text accompanying notes 39 and 43.

[26] *Olmstead*, 277 U.S. at 438.

[27] *Katz,* 389 U.S. at 351.

[28] United States v. Miller, 425 U.S. 435, 443 (1976); *Carpenter*, 138 S. Ct. at 2216 (attributing the origin of the third-party doctrine to the *Miller* case stating, "[t]his third-party doctrine largely traces its roots to *Miller*.").

[29] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[30] THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (1880) ("The right to one's person may be said to be a right of complete immunity: to be let alone.").

[31] Judge Cooley's "personal rights" included "right to life, the right to immunity from attacks and injuries, and the right equally with others similarly circumstanced to control one's own action," as well as right to reputation. *See id.* at 24.

[32] *Id.* at 64–65.

[33] *Id.* at 66.

[34] *Id.* at 32.

drew a distinction between libel as "rights of the individual"[35] and privacy as "the rights of the political community"[36] where unwanted publicity injures public morals and disturbs public peace.[37] Here, Judge Cooley's notion of privacy is more than suggesting a new tort, but a protection of the person as a mixture of both private law and public law order. This is consistent with his advocacy for constitutional protection of privacy in his work "Inviolability of Telegraphic Correspondence" in the *American Law Register*.[38]

In their celebrated article,[39] Samuel Warren and Louis Brandeis built their argument along the line of Judge Cooley, "as a part of the more general right to the immunity of the person—the right to one's personality."[40] They distinguished privacy from libel, for "the wrongs and correlative rights recognized by the law of slander and libel are in their nature material rather than spiritual."[41] They emphasized that "the rights, so protected, whatever their exact nature, are not rights arising from contract," nor "the principle of private property, unless that word be used in an extended and unusual sense."[42] For Warren and Brandeis, the essence of the right to privacy was "not the principle of private property, but that of an inviolate personality."[43]

---

[35] *Id*.

[36] *Id.*

[37] *Id.*

[38] *Inviolability of Telegraphic Correspondence*, 18 AM. L. REG. 65 (1879). The article was not marked, the authorship was attributed to Judge Cooley by his contemporary, Henry Hitchcock, in a paper read in August 1879 at an annual meeting of the American Bar Association. *See* Henry Hitchcock, *The Inviolability of Telegrams*, REP. SECOND ANN. MEETING AM. BAR ASS'N 93, 103 (1879). Judge Thomas M. Cooley pushed for the idea in his influential treatise, *Constitutional Limitations* (1868), where he elaborated on constitutional constraints on unreasonable searches and seizures under the Fourth Amendment. *See* THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS 299–308 (1868).

[39] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[40] *Id.* at 207.

[41] *Id.* at 197.

[42] *Id*. at 213.

[43] *Id*. at 205. "The right of property in its widest sense, including all possession, including all rights and privileges, and hence embracing the right to an violate personality, affords alone that broad basis upon which the protection which the individual demands can be rested." Warren & Brandeis, *supra* note 39, at 211. *See also* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. REV. 962, 971 (1964) (arguing "inviolate personality" is the "most significant indication of the interest [Warren and Brandeis] sought to protect" by the notion of right to privacy). After the 1890 Warren and Brandeis article, the most important contribution to the conversation surrounding privacy is by Dean Roscoe Pound. *See* Roscoe Pound, *Equitable Relief against Defamation and Injuries to Personality*, 29 HARV. L. REV. 640 (1916); Roscoe Pound, *Interests of Personality*, 28 HARV. L. REV. 343 (1915). Other scholars following this line of advocacy include Wilbur Larremore, *Law of Privacy*, 12 COLUM. L. REV. 694 (1912); Zechariah Chafee, Jr., *Progress of the Law 1919–1920*, 34 HARV. L. REV. 388, 407–14 (1921); Joseph R. Long, *Equitable Jurisdiction to Protect Personal Rights*, 33 YALE L.J. 115, 122–26 (1923) (discussing the right to privacy); Leon Green, *Right of Privacy*, 7 U. ILL. L. REV. 237 (1932).

The Warren and Brandeis article immediately caused a debate among state courts.[44] In the common law tradition up to this point, a person's name,[45] private letters, manuscripts, or drawings were protected as property.[46] The English Chancery Court acknowledged in *Prince Albert v. Strange* that "[u]pon the principle . . . of protecting property, it is that the common law . . . shelters the privacy and seclusion of thoughts and sentiments committed to writing, and desired by the author to remain not generally known."[47]

However, there were limits to the property theory. If letters were protected because they were mental labor, there was no reason why telegraphs were not protected in the same way. Likeness cases posed similarly tricky questions. For example, in *Pollard v. Photographic Company*,[48] plaintiff Allice Pollard's photograph was made into a Christmas card. The court noted, that when there was some right of property infringed, the law protected the "products of a man's own skill or mental labor." However, the court stated, "in the present case the person photographed has done nothing to merit such protection. . ."[49] An implied contract provided a solution in disputes between a customer and her photographer.[50] What happens where there is no contract? In *Schuyler v.*

---

[44] The New York Court of Appeals rejected the right of privacy in two widely noted cases. *See* Schuyler v. Curtis, 42 N.E. 22 (N.Y. 1895); Roberson v. Rochester Folding Box Co., 171 N.Y. 538, 64 N.E. 442 (N.Y. 1902). The New York legislature responded to the Court's decisions by passing a law, N.Y. Sess. Laws 1903, ch. 132, §§1–2, recognizing the right of privacy. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960). *See also* Atkinson v. Doherty & Co., 80 N.W. 285 (Mich. 1899) (describing how defendant, a manufacturer of cigars, sought to put on the market under a label bearing plaintiff's name and likeness). Rhode Island also rejected the right to privacy. Henry v. Cherry & Webb, 73 A. 97 (R.I. 1909) (noting plaintiff's pictures were used in commercial advertisements without consent).

[45] *See* Routh v. Webster (1847) 50 Eng. Rep. 698 (noting that injunction was granted enjoining defendants from using plaintiff's name in their corporate papers without consent); Dixon v. Holden, L.R. 7 Eq. 488 (1869) (granting plaintiff injunction against defendant from using plaintiff's name in an advertisement); Mackenzie v. Mineral Springs Co., 18 N.Y.S. 240 (1891) (plaintiff's name was used in advertisement); Brown Chem. Co. v. Meyer, 139 U.S. 540, 544 (1891) ("A man's name is his own property.").

[46] In personal letter cases, Gee v. Pritchard (1818) 36 Eng. Rep. 670, 678 ("I am of opinion, that the Plaintiff has a sufficient property in the original letters to authorize an injunction, unless she has by some act deprived herself of it."); Prince Albert v. Strange (1849) 41 Eng. Rep. 1171 (holding an injunction was granted against defendant publisher from publishing private drawings and etchings); Woolsey v. Judd, 11 N.Y.S. 379 (1855) (involving the publication of private letters without permission); Grigsby v. Breckinridge, 2 Bush 480 (Ky. 1867) (personal letters). However, there are exceptions. For example, when private letters fall into the hands of a stranger, that stranger can produce the letters voluntarily for court proceedings. *See* Barrett v. Fish, 47 A. 174 (Vt. 1899); *see also* Hopkinson v. Burghley, L. R. 2 Ch. 447 (1867).

[47] Prince Albert v. Strange, 2 De Gex & Smale 652, 695 (Ch. 1848).

[48] Pollard v. Photo. Co., 40 Ch. Div. 345 (Ch. 1888).

[49] *Id.* at 352.

[50] *Id.* at 349-50 ("I hold that the bargain between the customer and the photographer includes, by implication, an agreement that the prints taken from the negative are to be appropriated to the use of the customer only."). In a similar case in Minnesota, the Supreme Court of Minnesota followed the *Pollard* ruling. *See* Moore v. Rugg. 46 N.W. 141, 142 (Minn. 1890); *see also* Corliss v. E.W. Walker Co., 64 F. 280 (C.C.D. Mass. 1894).

Curtis, the defendants were members of "Woman's Memorial Fund Association," wishing to honor Mrs. Schuyler by erecting a statue and exhibiting it at the Columbian Exposition of 1893. Her relatives opposed, alleging injury of pain and disgrace, but not libel.[51] The New York Court of Appeal avoided the issue of privacy.[52] Seven years later, in *Roberson v. Rochester Folding Box Co.*, the defendant was a flour manufacturer who used the plaintiff's photographs in its advertisements.[53] There was no contract. No libel was alleged since the likeness was a good one.[54] This time, the Court of Appeals rejected the notion of privacy. Judge Gray's struggle continued. On the one hand, Judge Gray stated that "[t]he right of privacy, or the right of the individual to be let alone, is a *personal* right";[55] on the other, however, Judge Gray considered the notion of property "unduly restricted." Therefore, he argued for a broader concept of property that included privacy.[56]

Judge Gray's opinion was fully adopted by the Supreme Court of Georgia in its ruling in *Pavesich v. New England Life Insurance Co*.[57] *Pavesich* brought commercial appropriation cases into the framework of privacy,[58] which used to be under property.[59] What about non-commercial appropriation? In a New York case,[60] the plaintiff was arrested without a warrant, then photographed

---

[51] Schuyler v. Curtis, 147 N.Y. 434, 453 (1895) (rev'g Schuyler v. Curtis, 24 N.Y. Supp. 509 (Sup. Ct. 1893)).

[52] Judge John Clinton Gray embraced the idea of privacy by advocating a broad notion of property since he could not "see why the right of privacy is not a form of property." *Id.* (Gray, J., dissenting).

[53] Roberson v. Rochester Folding Box Co., 64 N.E. 442, 448 (N.Y. 1902).

[54] *Id.* at 450.

[55] *Id.* at 449–50 (Gray, J., dissenting) (emphasis added).

[56] Judge Gray stated:

Property is not, necessarily, the thing itself, which is owned; it is the right of the owner in relation to it. The right to be protected in one's possession of a thing, or in one's privileges, belonging to him as an individual, or secured to him as a member of the commonwealth, is property, and as such entitled to the protection of the law. *Id*. at 451 (Gray, J., dissenting).

[57] Pavesich v. New England Life Ins. Co., 50 S.E. 68, 78 (Ga. 1905) (holding a property violation when plaintiff's photograph was used without consent by defendant insurance company in an advertisement on newspaper).

[58] Foster-Milburn Co. v. Chinn, 120 S.W. 364, 366 (Ky. 1909) (holding a privacy violation when a pharmaceutical company forged and published a recommendation of a medicine using the name and picture of the plaintiff without consent. The Supreme Court of Kentucky ruled that "we concur with those holding that a person is entitled to the right of privacy as to his picture . . ."); *see also* Douglas v. Stokes, 149 S.W. 849 (Ky. 1912) (holding a privacy violation when the defendant photographer, who was employed by parents to photograph the nude body of a deformed child, copyrighted and published the photograph without consent).

[59] Atkinson v. Doherty & Co., 80 N.W. 285 (Mich. 1899) (holding that defendant, a manufacturer of cigars, who sought to put cigars on the market under a label bearing plaintiff's name and likeness, was not a privacy violation). The Rhode Island Supreme Court continued this approach after the *Pavesich* decision, *see*, Henry v. Cherry & Webb, 73 A. 97 (R.I. 1909) (holding a privacy violation when plaintiff's pictures were used in commercial advertisements without consent).

[60] Owen v. Partridge, 82 N.Y.S. 248 (1903).

and fingerprinted at the police station. The next morning, he was discharged for lack of evidence. Plaintiff moved for a preliminary injunction to have his photograph and measurements eradicated. The New York County court could only deny Owen's motion since New York did not recognize the right of privacy.[61] In a Maryland case, the defendant hired a detective to follow the plaintiff wherever he should go. Plaintiff asked the court for an injunction, but the court refused, claiming that there was no property to protect.[62]

2. The Turn to Property

In the 1920s, the government expanded its powers by collecting data from citizens, in tax,[63] securities,[64] labor relations,[65] and communications.[66] A commentator wrote in 1926, "[i]n the last few decades hundreds upon hundreds of governmental agencies have been created by Congress and the state legislatures, most of them expressly granted this far-reaching power over the liberty of the citizen."[67] It was in the prohibition period that the United States Supreme Court in *Olmstead v. United States* (1928) ruled that wiretapping was not a "search" under the Fourth Amendment.[68] In this case, three telephone companies and a trade association filed an amicus brief,[69] arguing that wiretapping "violates the property rights of both persons then using the

---

[61] In two similar cases in Louisiana, the Louisiana Supreme Court ruled in favor of privacy. *See* Itzkovitch v. Whitaker, 42 So. 228, 229 (La. 1906); Schulman v. Whitaker, 42 So. 227, 228 (La. 1906).

[62] Chappell v. Stewart, 33 A. 542, 542–43 (Md. 1896).

[63] *See* The Revenue Act of 1918, Pub. L. No. 065-254, § 1305, 40 Stat. 1057 (1918) (providing: "[t]he Commissioner, for the purpose of ascertaining the correctness of any return or for the purpose of making a return where none has been made, is hereby authorized, by any revenue agent or inspector designated by him for that purpose, to examine any books, papers, records or memoranda bearing upon the matters required to be included in the return, and may require the attendance of the person rendering the return or of any officer or employee of such person . . ."); *see also* United States v. First Nat'l Bank of Mobile, 295 F. 142 (S.D. Ala. 1924), *aff'd*, 267 U.S. 576 (1925); Brownson v. United States, 32 F.2d 844 (8th Cir. 1929).

[64] *See* Securities Act of 1933, Pub. L. No. 73-22, § 8(e), 48 Stat. 74 (1933) (empowering the Securities Exchange Commission (SEC)); *see also* McGarry v. SEC, 147 F.2d 389 (10th Cir. 1945).

[65] *See* Fair Labor Standards Act of 1938, Pub. L. No. 75-718, ch. 676, 52 Stat. 1060 (1938) (Section 9 describes government's power to carry out hearing and investigation, includes production of books, papers, and documents, and incorporates sections 9 and 10 of the Federal Trade Commission Act of 1914, Pub. L. No. 63-203, ch. 311, 38 Stat. 717 (1914).); *see also* Okla. Press Publ'g Co. v. Walling, 327 U.S. 186 (1946).

[66] Federal Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934).

[67] *See* David E. Lilienthal, *The Power of Governmental Agencies to Compel Testimony*, 39 HARV. L. REV. 694, 696–97 (1926); *see also* Foster H. Sherwood, *The Enforcement of Administrative Subpoenas*, 44 COLUM. L. REV. 531 (1944).

[68] Olmstead v. United States, 277 U.S. 438 (1928).

[69] Pacific Telephone and Telegraph Company, American Telephone and Telegraph Company, and the Tri-State Telephone and Telegraph Company and also a trade association (United States Independent Telephone Association). *Olmstead*, 277 U.S. at 452–54; *see* Zechariah Chafee, Jr., *Progress of the Law 1919–1920*, 34 HARV. L. REV. 388 (1921).

telephone, and of the telephone company as well."[70] They asked, "does not wiretapping involve an 'unreasonable search,' of the 'house' and of the 'person'?"[71] The Court agreed in principle, but found no trespass, insisting that "[t]here was no entry of the houses or offices of the defendants."[72] The *Olmstead* Court held that "[t]he language of the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office."[73] Brandeis, now an Associate Justice on the Supreme Court, dissented from the majority. Brandeis firmly believed that "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[74]

3. The "New Property"

By the 1950s, there were growing concerns about privacy.[75] A meticulous report, known as the Dash Report, detailed the widespread use of surveillance and invasion of citizens' privacy.[76] Without warrant or consent, welfare agency officers visited citizens' homes for inspection purposes.[77] The most outrageous

---

[70] *Olmstead*, 277 U.S. at 453.

[71] *Id.*

[72] *Id.* at 464.

[73] *Id.* at 465.

[74] *Id.* at 478 (Brandeis, J., dissenting); *see also* Leon Green, *Right of Privacy*, 27 ILL. L. REV. 237, 238 (1932) (arguing that "the interests involved in the 'privacy' cases belong to the group classed as *interests of personality*, rather than to the group of *property interests* or that of *interests in relations with other persons*."); Louis Nizer, *Right of Privacy—A Half Century's Developments*, 39 MICH. L. REV. 526 (1941).

[75] *See, e.g.*, *Wiretapping, Eavesdropping, and the Bill of Rights: Hearing before the Subcomm. on Const. Rights of the Comm. on the Judiciary,* 85th Cong. (1958) (Part 1); Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Proposal*, 52 COLUM. L. REV. 165 (1952); Richard C. Donnelly, *Comments and Caveats on the Wire Tapping Controversy*, 63 YALE L.J. 799 (1954); Floyd E. Siefferman, Jr., Note, *Interception in Telephonic Communications under Section 605 of the Federal Communications Act*, 8 J. PUB. L. 318 (1959); Daniel J. Dykstra, *The Right Most Valued by Civilized Man*, 6 UTAH L. REV. 305, 305–06 (1959) ("[T]here are currently operative forces which seriously threaten to alter the historic relationship of the individual to government and to society."); Note, *Judicial Control of Illegal Search and Seizure*, 58 Yale L.J. 144 (1948). In 1946, the New York State Bar Association commissioned a study on the issue of wiretapping. *See also* Margaret Lybolt Rosenzweig, *Law of Wire Tapping I*, 32 CORNELL L. Q. 514 (1947); and *Law of Wire Tapping II*, 33 CORNELL L. Q. 73 (1947); *and* FREDERICK F. GREENMAN, WIRE-TAPPING, ITS RELATION TO CIVIL LIBERTIES (1938).

[76] SAMUEL DASH ET AL., THE EAVESDROPPERS (1959); *see* Thomas C. Hennings, Jr., et al., *The Wiretapping-Eavesdropping Problem: Reflections on The Eavesdroppers*, 44 MINN. L. REV. 808 (1960).

[77] *See* Frank v. Maryland, 359 U.S. 360 (1959) for a case where a city health inspector requested homeowner's permission to inspect his basement. The homeowner refused and was arrested for violation of city's health code. The Supreme Court ruled that the health code did not violate the Due Process Clause of the Fourteenth Amendment.

example was the midnight mass raids by welfare agencies in the early 1960s.[78] The year 1967 marked a significant change. In June, the Supreme Court brought the administrative entry of homes under the framework of the Fourth Amendment.[79] One week later, in *Berger v. New York*,[80] the Court ruled that evidence obtained by eavesdropping via a recording device in an attorney's office violated the Fourth Amendment for trespassory intrusion into a constitutionally protected area. Further, in *Katz v. United States* (1967),[81] the Court ruled that wiretapping without a warrant, in a public telephone booth, violated the Fourth Amendment. *Katz* prompted Congress to enact Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[82] which outlawed wiretapping by private parties and required a search warrant for authorized wiretapping. Conceptually, the *Katz* Court departed from the property-based framework in *Olmstead*, and announced that "the Fourth Amendment protects people, not places."[83] The Court declared that the "trespass" doctrine "can no longer be regarded as controlling."[84] Instead, the *Katz* court imagined privacy right as legal protection for a person:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[85]

If this was still vague, Justice Harlan's formula in his concurring opinion in *Katz* provided two requirements: first, that a person has exhibited an actual

---

[78] Charles A. Reich, *Midnight Welfare Searches and the Social Security Act*, 72 YALE L.J. 1347, 1347 (1963) ("In many states, and in the District of Columbia, it has become common practice for authorities to make unannounced inspections of the homes of persons receiving public assistance. Often such searches are made without warrants and in the middle of the night."). It was not until 1967 that the Supreme Court of California declared the mass raids unconstitutional. *See* Parrish v. Civ. Serv. Comm'n Alameda C'nty, 425 P.2d 223 (Cal. 1967) (*en banc*).

[79] Camara v. Mun. Ct. of S.F., 387 U.S. 523 (1967) (holding that the Fourth Amendment barred prosecution of a person who has refused to permit a warrantless inspection of his residence in accordance with the Housing Code of San Francisco); *see also* See v. Seattle, 387 U.S. 541 (1967) (holding that the Fourth Amendment bars prosecution of a person who has refused to permit a warrantless inspection of his residence in accordance with Seattle's Fire Code).

[80] Berger v. New York, 388 U.S. 41, 64 (1967).

[81] Katz v. United States, 389 U.S. 347, 359 (1967).

[82] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968), (codified at 34 U.S.C. §§ 10101 et seq. (2020)). Two decisions by the Supreme Court were key to the 1968 Act: *Katz*, and *Berger v. United States*, 388 U.S. 41 (1967). *See* Louis Fisher, *Congress and the Fourth Amendment*, 21 GA. L. REV. (SPECIAL ISSUE) 107, 152 (1986).

[83] *Katz*, 389 U.S. at 351.

[84] *Id.* at 353.

[85] *Id.* at 351–52. Proposals for the personality approach, *see* Charles A. Reich, *The New Property*, 73 YALE L.J. 733 (1964); Sanford H. Kadish, *Methodology and Criteria in Due Process Adjudication—A Survey and Criticism*, 66 YALE L.J. 319, 347 (1957) (discussing the notion of man's dignity and its procedural safeguards, including the respect for privacy); Bloustein, *supra* note 43.

(subjective) expectation of privacy; and second, that that expectation is one that society is prepared to recognize as "reasonable."[86]

Despite its potential, *Katz* did not lead to a broad revolution in the notion of privacy. Governments continued collecting data from citizens.[87] With the introduction of computers in the 1960s, Alan F. Westin observed that ". . . the 1960s witnessed wide public anxiety over what has come to be called the 'databank issue'—an amalgam of concerns about the extent and uses of record-keeping by organizations, their move to computers, and possible effects of computerization on rights of personal privacy."[88]

4. Third-Party Property

More importantly, another line of thinking based on property gained currency in courts—the third-party doctrine. The doctrine was developed in the context where federal agencies were increasingly granted the power to collect data from third parties. In *United States v. First National Bank of Mobile* (1924),[89] a federal court ruled that the Bureau of Internal Revenue had the right to request a commercial bank produce information about its customers. The bank refused to testify and produce the books based on the Fourth Amendment. The court suggested that the Fourth Amendment did not extend to a "third party."[90] In subsequent years, federal courts repeatedly upheld administrative subpoenas issued by the IRS to banks, accountants, lawyers, and even hospitals for information about their customers, clients, or

---

[86] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[87] Census was one contentious area at the time. Courts consistently upheld laws on census, before and after the *Katz* ruling. Before *Katz*, see United States v. Rickenbacker, 197 F. Supp. 924 (S.D.N.Y. 1961), *aff'd*, 309 F.2d 462 (2nd Cir. 1962), *cert. denied*, 371 U.S. 962 (1963). The *Rickernbacker* case was referred to with approval by the majority of the United States Supreme Court in Wyman v. James. 400 U.S. 309 (1971). After *Katz*, see United States v. Little, 321 F. Supp. 388 (D. Del. 1971); United States v. Steele, 461 F.2d 1148 (9th Cir. 1972).

[88] ALAN F. WESTIN, DATABANKS IN A FREE SOCIETY 4 (1972). *See also* ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971); Symposium, *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211 (1968); Arthur R. Miller, *The Dossier Society*, 1971 U. ILL. L.F. 154 (1971); Stanley P. Wagner, *Records and the Invasion of Privacy*, 40 SOC. SCI. 38 (1965).

[89] United States v. First Nat'l Bank of Mobile, 295 F. 142 (S.D. Ala. 1924), *aff'd*, 267 U.S. 576 (1925) (relying on grand jury subpoena cases, suggesting that the Supreme Court considered that federal agencies had the same subpoena power as the federal grand jury).

[90] 295 F. at 143. Similarly, in *Newfield v. Ryan*, a unanimous Fifth Circuit upheld SEC's subpoena on Western Union, the telegraph company, for telegrams sent and received by plaintiff Ryan Florida Corporation. The Fifth Circuit considered the telegrams property of the Western Union, not that of the customers: "the subpoenas do not take plaintiff's property, nor invade their right of privacy in the messages, inspection of which is demanded." Newfield v. Ryan, 91 F.2d 700, 703 (5th Cir. 1937).

patients.[91] In *Donaldson v. United States*,[92] the Supreme Court provided further clarity. Here, in its investigation of petitioner's tax returns, the IRS issued summonses to petitioner's former employer and its accountant for their records of petitioner's employment and compensation during the period of investigation. A unanimous Supreme Court affirmed the lower court's decision and ruled that there was no violation of the Fourth Amendment. The Court reiterated in its opinion that,

> [e]ach of the summonses here, we repeat, was directed to a *third person* with respect to whom no established legal privilege, such as that of attorney and client, exists, and had to do with records in which the taxpayer has no proprietary interest of any kind, which are owned by the third person, which are in his hands, and which relate to the third person's business transactions with the taxpayer.[93]

The ultimate clarity was found in *United States v. Miller*.[94] In an investigation of the illegal possession of liquor, a grand jury issued subpoenas duces tecum to two commercial banks for records of accounts owned by Miller.[95] Without advising Miller of the subpoenas, the two banks produced the records—microfilm records of Miller's account, one deposit slip, and one or two checks.[96] Miller challenged the subpoenas and alleged the bank records were illegally seized.[97] The Court's decision was based on a different statute—the Bank Secrecy Act of 1970—but its reasoning closely followed the logic of

---

[91] First Nat'l Bank of Mobile v. United States, 160 F.2d 532 (5th Cir. 1947); Falsone v. United States, 205 F.2d 734 (5th Cir. 1953) (holding a public certified accountant must produce taxpayers' books and records, even though the relationship between taxpayers and accountant was confidential); *In re* Albert Lindley Lee Mem'l Hosp., 209 F.2d 122 (2nd Cir. 1953) (noting that names and addresses of patients confined in the hospital were not privileged); Chapman v. Goodman, 219 F.2d 802 (9th Cir. 1955); Sale v. United States, 228 F.2d 682 (8th Cir. 1956); Hubner v. Tucker, 245 F.2d 35 (9th Cir. 1957); Foster v. United States, 265 F.2d 183 (2nd Cir. 1959); Bouschor v. United States, 316 F.2d 451 (8th Cir. 1963); United States v. Cont'l Bank & Trust Co., 503 F.2d 45 (10th Cir. 1974). For contemporary commentaries, see Note, *The Power of the Bureau of Internal Revenue to Subpoena Books and Records in Tax Investigations*, 1958 WASH. U. L. REV. 277; A. Sherwood Godwin, Jr., *Constitutional Law—Attorney's Rights under Fifth Amendment to Withhold Client's Tax Records from Internal Revenue Service*, 9 WAKE FOREST L. REV. 561 (1973); Lynn Katherine Thompson, *IRS Access to Bank Records; Proposed Modifications in Administrative Subpoena Procedure*, 28 HASTINGS L.J. 247 (1976).

[92] Donaldson v. United States, 400 U.S. 517 (1971).

[93] *Id.* at 523 (emphasis added).

[94] United States v. Miller, 425 U.S. 435 (1976); Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) ("This third-party doctrine largely traces its roots to *Miller*."); Bradford P. Wilson, *Enforcing the Fourth Amendment: A Jurisprudential History*, 28 CATH. LAW. 173 (1986).

[95] *Miller*, 425 U.S. at 440.

[96] *Id.* at 438.

[97] *Id.* In 1973, when he filed his notice of appeal to the Fifth Circuit, Miller relied on Stark v. Connally, 347 F. Supp. 1242 (N.D. Cal. 1972), where a three-judge panel ruled that certain provisions in the Bank Secrecy Act of 1970 were in violation of the Fourth Amendment. However, the U.S. Supreme Court later reversed the rulings of the district court on the Fourth Amendment, see California Bankers Association v. Shultz, 416 U.S. 21 (1974).

Donaldson. The *Miller* Court also emphasized the issue of who owned the bank records: "the documents subpoenaed here are not respondent's 'private papers.'" [98] Rather, the Court reasoned, "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[99]

In *Whalen v. Roe*,[100] a unanimous Supreme Court upheld New York State legislation requiring patient identification information to be filed with the New York State Department of Health to control dangerous legitimate drugs. The Court held that the "requirement was a reasonable exercise of the State's broad police powers" and did not constitute an invasion of any right or liberty protected by the Fourteenth Amendment.[101] The Court added some final words to show that it was "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[102]

In the area of telecommunications, whether dialing records from the telephone companies were under the protection of the Fourth Amendment became a contentious issue. The pen register—a device that records dialing information—was introduced in the 1950s,[103] and by the mid-1960s, it had been frequently used by police to record telephone numbers dialed on the line.[104] Though it did not have any capacity to record the content of a phone conversation,[105] law enforcement quickly found it helpful. *United States v. New*

---

[98] *Miller*, 425 U.S. at 440.

[99] *Id.* at 442.

[100] Whalen v. Roe, 429 U.S. 589 (1977).

[101] *Id.* at 598.

[102] *Id.* at 605.

[103] An early case was Schmukler v. Ohio-Bell Tel. Co., 116 N.E.2d 819 (Cuyahoga Cnty. C.P. 1953), where a telephone company installed a pen register to track telephone callings of a customer based on the company's suspicion of misuse of their service. The customer sued for a violation of privacy. The Court found for the telephone company, holding that "by their agreement and under the law the defendant [telephone company] had the right and duty to supervise its service and the right and duty to investigate suspicious misuse of said service." *Id.* at 826.

[104] The first appearance of a pen register in congressional hearings was in May 1965, when Lee Loevinger, Commissioner of the Federal Communications Commission, appeared before the Subcommittee on Administrative Practices and Procedure of the Senate Committee on the Judiciary. *See Invasions of Privacy (Government Agencies): Hearings Before the Subcomm. on Admin. Prac. and Proc. of the Comm. on the Judiciary,* 89th Cong. 954–62 (1965) (explaining the design and functions of pen register). In January 1968, in a testimony before a House Committee by Hubert Kertz, Operating Vice President of AT&T, the pen register was explained as a device to record abusive callings. *See Hearing Before the Subcomm. on Commc'ns and Power of the Comm. on Interstate and Foreign Com.,* 90th Cong. 17–23 (1968).

[105] *Hearing Before the Subcomm. on Commc'ns and Power of the Comm. on Interstate and Foreign Com., 90th Cong.* at 21. Hubert Kertz told the House Committee in 1968, "[T]here is nothing about these devices or methods that involve any monitoring of conversations of either the calling or the

York Telephone Co.,[106] answered the question of whether a federal district court may properly direct a telephone company to provide federal law enforcement officials the facilities and technical assistance for installing pen registers in their investigation of crimes without a warrant. The Supreme Court concluded that "[p]en registers do not 'intercept' because they do not acquire the 'contents' of communications."[107] Less than two years later in *Smith v. Maryland*,[108] a convicted defendant raised the same question. In *Smith*, the Court ruled that a pen register was not a "search" under the Fourth Amendment; therefore, it was lawful for law enforcement to install a pen register at the telephone company's central offices to collect dialing information without a warrant.[109] The Court reiterated that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[110]

These decisions show that prior to the arrival of the internet, the United States Supreme Court had already developed its framework of the notion of privacy defined by data collector's property (DCP). The arrival of the internet and social media poses questions about whether legal doctrines that developed in the analog age still apply in the digital era.[111] Anonymity in cyberspace was both celebrated and feared in the early stages of the internet;[112] however, it is now illusory in surveillance capitalism.[113]

called person's telephone line. There is no attempt whatsoever to listen to conversations. It is simply a matter of identifying the calling line." *Id.*

[106] United States v. New York Tel. Co., 434 U.S. 159 (1977). Before the Supreme Court decision, the pen register had received attention in federal courts. *See* Victor S. Elgort, Note, *Legal Constraints Upon the Use of the Pen Register as a Law Enforcement Tool*, 60 CORNELL L. REV. 1028 (1975); Robert B. Parrish, Note, *Circumventing Title III: The Use of Pen Register Surveillance in Law Enforcement*, 1977 DUKE L.J. 751 (1977).

[107] *New York Tel. Co.,* 434 U.S. at 167.

[108] Smith v. Maryland, 442 U.S. 735 (1979).

[109] *Id.* at 746.

[110] *Id.* at 741.

[111] Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553 (2016) (arguing that the traditional conceptual distinctions between public and private space, personal and third-party information, content and non-content, domestic and international, fundamental to the Fourth Amendment, have been undermined in the digital world); naturally, scholars debated about the third-party doctrine in the new context, *e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009).

[112] Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639 (1995) (Symposium: Emerging Media Technology and the First Amendment); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L. J. 869 (1996).

[113] BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLE TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015) ("In the age of ubiquitous surveillance, where everyone collects data on us all the time, anonymity is fragile . . . .").

B. The Return to Property

The third DSP offensive—led by Lessig and Balkin, among others—however, was overshadowed by two other factors: the September 11 attack, as well as the rise of social media. Digital platforms emerged as the most rapidly expanding data collectors. The Roberts Court brought the third-party doctrine into cyberspace through their rulings in *United States v. Jones*, [114] and *Carpenter v. United States*.[115] A crucial character of this third-party doctrine in cyberspace is its narrow notion of privacy through legal analysis that focuses on the particular technology in question, and its ruling that tends to be piecemeal and binary. This character becomes clearer in comparison with the jurisprudence of the Court of Justice of the European Union that is more interested in articulating constitutional principles and providing guidelines to legislatures, as will be discussed in Part III.

In *United States v. Jones*,[116] the Justices were in agreement with each other on the conclusion that attaching a GPS device and using it to track the location information constituted a search under the Fourth Amendment, thereby a search warrant was required. The differences between the majority and concurring opinions were the rationales underlying that conclusion. Justice Scalia, writing for the majority that included Chief Justice Roberts and Justices Kennedy, Thomas, and Sotomayor, rejected *Katz* bluntly.[117] Justice Scalia declared, "Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation." [118] In its place, Justice Scalia reinstated trespass-based privacy: "for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas . . . it enumerates."[119]

Justice Sotomayor was puzzled by this approach. For her, this was totally out of touch with reality in cyberspace.[120] Justice Sotomayor considered the trespassory test the minimum;[121] more importantly, according to Sotomayor,

---

[114] United States v. Jones, 565 U.S. 400 (2012).

[115] *Carpenter,* 138 S.Ct. at 2222.

[116] *Jones,* 565 U.S. at 400.

[117] *Id.*

[118] *Id.* at 406.

[119] *Id.*

[120] In her concurring opinion, Justice Sotomayor found that "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance." *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring). For commentaries on Justice Sotomayor's opinion, see Miriam H. Baer, *Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes out Middle Ground in United States v. Jones*, 123 YALE L.J. F. 393 (2014).

[121] *Jones*, 565 U.S. at 414 (Sotomayor, J., concurring) ("[T]he trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case.").

the Fourth Amendment was broader. The test, Justice Sotomayor hinted, should not be based on property, but on the effect on the person—whether collecting the data may "alter the relationship between citizen and government in a way that is inimical to democratic society."[122] Justice Sotomayor's view was closer to the DSP data theory, but she was a lone voice on the bench. Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, shared Justice Sotomayor's critique of the trespassory test, believing that "an actual trespass is neither necessary *nor sufficient* to establish a constitutional violation."[123] Critical of *Katz* for letting judges make decisions about an expectation of privacy, Justice Alito believed that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[124]

C. Cell-site Location Information

Cell-site location information (CSLI) is records generated when cell phones are connected to radio antennas installed on cellular towers of the wireless service company. CSLI was at the center of the case in *Carpenter v. United States*.[125]

Here, in a robbery case, Detroit police sought disclosure of certain telecommunication records from wireless carriers MetroPCS and Sprint under the Stored Communications Act, 18 U.S.C. §2703(d). Federal magistrate judges issued two court orders, allowing the government to have access to, respectively, 127 days and 88 days of CSLI data.[126] The data was used in court to prove the defendants' whereabouts when the robbery happened. Defendants moved to suppress the CSLI data, alleging Fourth Amendment rights. The trial court denied the defendants' motion in 2013,[127] and in 2016, the Sixth Circuit affirmed.[128] The Sixth Circuit considered two fundamental factors: the primary factor was that CSLI data was *not* content but metadata,[129] and secondly, that

---

[122] *Id.* at 416.

[123] *Id.* at 423 (Alito, J., concurring).

[124] *Id.* at 429.

[125] United States v. Carpenter, 138 S.Ct. 2206 (2018).

[126] There is a slight disparity in the quantity of CSLI data in the records. The Supreme Court opinion suggested 127 days and 7 days, *Carpenter,* 138 S. Ct. at 2212, while the Sixth Circuit opinion suggested 127 days and 88 days, United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016).

[127] United States v. Carpenter, 2013 WL 6385838 (E.D. Mich. 2013), unpublished report (Criminal Case No. 12–20218), *aff'd* United States v. Carpenter, 926 F.3d 313 (6th Cir. 2019), rehearing was denied, 788 Fed.Appx. 364 (Mem) (6th Cir. 2019).

[128] United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), r*ev'd*, 138 S. Ct. 2206 (2018).

[129] *Carpenter*, 819 F.3d at 887 ("The Fourth Amendment protects the content of the modern-day letter, the email. But courts have not yet [at least] extended those protections to the internet analogue to envelop markings, namely the metadata used to route internet communications . . .") (citation omitted).

CSLI was a business record that Carpenter shared with his wireless carrier.[130] Guided by *Smith* as "the binding precedent," the Sixth Circuit ruled that Carpenter had no reasonable expectation for CSLI data privacy.[131]

The United States Supreme Court, however, reversed. Chief Justice Roberts, writing for the majority, stated that "[t]he location information obtained from Carpenter's wireless carriers was the product of a search."[132] The majority held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[133] In reaching the conclusion, the *Carpenter* majority did not address the content and non-content distinction—nor did the dissenting opinions. Instead, both the majority and dissenters focused on the third-party doctrine. While still recognizing third-party doctrine as a general rule, the majority's focused on explaining that CSLI data is a "qualitatively different category" of business records.[134] Following the recognition of the power of modern technology in *Jones* and *Riley*, the majority recognized that "when the Government tracks the location of a cell phone it achieves near perfect surveillance"[135] and that CSLI data "present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*."[136] Throughout the opinion, the majority emphasized the contrast between CSLI and traditional police tools:

> Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today.[137]

---

[130] *Id.* at 889 ("This case involves business records obtained from a third party, which can only diminish the defendants' expectation of privacy in the information those records contain.").

[131] The Sixth Circuit was the first federal circuit court applying the third-party doctrine to CSLI. United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004) (holding that defendant "had no legitimate expectation of privacy in the cell-site data because the DEA agents could have obtained the same information by following Garner's car."). Other circuit courts followed, *see, e.g., In re* U.S. for an Ord. Directing a Provider of Elec. Commc'n Serv. to Disclose Recs. to the Gov't, 620 F.3d 304, 313 (3rd Cir. 2010); *In re* Applic. of the U.S. for Hist. Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (*en banc*); United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (*en banc*); United States v. Thompson, 866 F.3d 1149 (10th Cir. 2017).

[132] *Carpenter*, 138 S.Ct. at 2217.

[133] *Id.*

[134] *Id.* at 2216–17 ("[W]hile the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records.").

[135] *Id.* at 2218.

[136] *Id.*

[137] *Carpenter*, 138 S.Ct. at 2219.

This way, the majority could keep the third-party doctrine as a general rule,[138] but declare that Carpenter had a reasonable expectation of privacy over his CSLI data.

Three of the dissenting justices believed that the cellphone company owned the data: "The records were the business entities' records, plain and simple."[139] "Cell-site records . . . are created, kept, classified, owned, and controlled by cell phone service providers[.]" [140] Justice Thomas dissented and reiterated that "the Government did not search Carpenter's property."[141] Justice Gorsuch, who voted against protecting CSLI data, entertained the idea of bailment—that cellphone users owned the data but entrusted the cellphone company to manage them.[142] Justice Gorsuch's bailment theory does not appear as a direct denial of DSP rights; nevertheless, it came to the same conclusion.

Tech firms welcomed the *Carpenter* ruling,[143] and advocacy groups hailed the ruling as a victory for privacy.[144] However, others are more cautious.[145] Professor Susan Freiwald and former Magistrate Judge Stephen Wm. Smith considered it an achievement that the *Carpenter* Court "significantly narrowed the [third-party] doctrine's scope"[146] and that it "marks the first time the Court has explicitly announced the possibility of reasonable expectations of privacy

---

[138] *Id.* ("The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.").

[139] *Id.* at 2228.

[140] *Id.* at 2229 (Kennedy, J., dissenting).

[141] *Id.* at 2235 (Thomas, J., dissenting).

[142] *Id.* at 2268 (Gorsuch, J., dissenting).

[143] *See* Brief for Technology Companies as Amici Curiae in Support of Neither Party at 1, Carpenter v. United States, 138 S.Ct. 2206 (2018) (No. 16-402), 2017 WL 3601390, at *1–2 ("Rigid rules such as the third-party doctrine and the content/non-content distinction make little sense in the context of digital technologies and should yield to a more nuanced understanding of reasonable expectations of privacy, including consideration of the sensitivity of the data and the circumstances under which such data is collected by or disclosed to third parties as part of people's participation in today's digital world") (Filing of appellate brief by Airbnb, Apple, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest Labs, Oath, Snap, Twitter, and Verizon).

[144] *See* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J. L. & TECH. 357, 387 (2019); *see also* Nicholas A. Kahn-Fogel, Katz, Carpenter*, and Classical Conservatism*, 29 CORNELL J.L. & PUB. POL'Y 95, 151 (2019); Eunice Park, *Objects, Places and Cyber-Spaces Post-*Carpenter*: Extending the Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA*, 21 YALE J. L. & TECH. 1, 58 (2019); Alan Z. Rozenshtein, *Fourth Amendment Reasonableness after* Carpenter, 128 YALE L. J. F. 943, 960 (2019); Susan Freiwald*, Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 748–49 (2011); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now? Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L. J. 117, 194–95 (2012); Christopher J. Borchert et. al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 64–65 (2015).

[145] Susan Freiwald & Stephen Wm. Smith, Commentary, *The Carpenter Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 205–35 (2018).

[146] *Id.* at 224.

in records stored with a third party."[147] But they also pointed out the long delay leading to this ruling: ten years since magistrate judges raised the issue and called for guidance, and twenty four years since Congress had signaled that CSLI data is entitled to greater legal protection.[148] Furthermore, the Court was explicit about limiting its ruling to seven days of historical CSLI.[149] What about real-time CSLI? Other data? Those issues would have to wait for another day in court.[150]

D. Photos in the Cloud

The internet's capacity to foster child pornography is an increasing concern.[151] In March 1998, the CyberTipline Program was launched through a Congressional mandate to receive reports regarding child sexual exploitation.[152] The Program is based on the "private search" doctrine that enables a private party who accidentally discovers child pornography to turn over the evidence to police.[153] In cyberspace, however, technology changes the

---

[147] *Id.* at 226.

[148] *See id.* at 231.

[149] The Court asserted the ruling's limitations:

> We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.

Carpenter, 138 S. Ct. at 2220.

[150] In subsequent cases, courts refused to extend the *Carpenter* ruling to new areas. *See* Commonwealth of Pennsylvania v. Dunkins, 263 A.3d 247 (Pa. 2021) (involving wireless internet network (WiFi) connection records obtained by police without warrant).

[151] *Online Child Pornography: Hearing Before the Comm. on Com., Sci. and Transp.*, 109th Cong. 1154 (2006).

[152] Missing, Exploited, and Runaway Children Protection Act, Pub. L. No. 106-71, 113 Stat. 1035 (1999) (codified as amended at 34 U.S.C. § 11291); *National Center for Missing and Exploited Children*, OFF. JUV. JUST. & DELINQ. PREVENTION, https://ojjdp.ojp.gov/programs/national-center-missing-and-exploited-children (last visited Sept. 22, 2022). The National Center for Missing and Exploited Children (NCMEC) gathers leads and tips regarding suspected online crimes against children and forwards them to the appropriate law enforcement agencies through its Congressionally mandated CyberTipline. *See CyberTipline*, NCMEC, https://www.missingkids.org/gethelpnow/cybertipline.

[153] United States v. Runyan, 275 F.3d 449 (5th Cir. 2001) (entering into the defendant's ranch, defendant's wife found and forwarded to police a desktop computer, floppy disks, CDs, and ZIP disks, which contained child pornography images); Rann v. Atchison, 689 F.3d 832 (7th Cir. 2012) (discovering the material, defendant's biological daughter brought a zip drive and camera memory card to police); United States v. Tosti, 733 F.3d 816 (9th Cir. 2013) (finding child pornography on defendant's computer when he brought it to a CompUSA store for service, employees of the store shared with police); United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015) (seeing child pornography images on defendant's laptop, his girlfriend shared the information with police); United States v. Fall, 955 F.3d 363 (4th Cir. 2020) (discovering child pornography, defendant's niece took defendant's laptop to police).

dynamics—it is more likely that the internet service provider discovers and reports child pornography to the police. In 2002, America Online (AOL) pioneered the use of the hash value in a detecting file through its Image Detection and Filtering Process (IDFP) and began to use it to detect child pornography in its users' email accounts.[154] Hash-value matching seemed to be a promising technique.[155] In 2006, the Technology Coalition, a group of leaders in the Internet services sector, and the National Center for Missing & Exploited Children (NCMEC) joined forces to help address this growing problem, and an idea was born.[156] In October 2008, Congress passed a law requiring internet service providers to report to CyberTipline any individual suspected of breaking federal law.[157] Google developed its CSAI (Child Sexual Abuse Imagery) Match for its YouTube content.[158] In 2009, Microsoft developed PhotoDNA technology and made it available in 2015 as a service on Azure, Microsoft's cloud service.[159] The question remained, however, of how to apply the private search doctrine to cyberspace.

1. The Private Search Doctrine

The legal doctrine of "private search" was announced by the United States Supreme Court in *United States v. Jacobsen*[160] and *Walter v. United States*.[161] In *Jacobsen*, Federal Express (FedEx) employees at the Minneapolis-St. Paul Airport opened a package (a cardboard box wrapped in brown paper) and discovered white powder. They reported this to the Drug Enforcement Administration (DEA).[162] Justice Stevens, writing for the majority, stated that the initial invasion of the package by employees of a private company "did not

---

[154] United States v. Richardson, 607 F.3d 357, 363 (4th Cir. 2010) (noting that AOL developed and deployed IDFP in 2002). AOL's pioneering work is recognized in T. J. McIntyre, *Child Abuse Images and Cleanfeeds: Assessing Internet Blocking Systems in* RESEARCH HANDBOOK ON GOVERNANCE OF THE INTERNET 277, 288 (2013).

[155] Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. F. 38 (2005); Mohammad Peyravian et al., *On Probabilities of Hash Value Matches*, 17 COMPUT. & SEC. 171 (1998).

[156] John Shehan, *Eliminating Child Sexual Abuse Material: The Role and Impact of Hash Values*, THORN BLOG (Apr. 18, 2016), https://www.thorn.org/blog/eliminating-child-sexual-abuse-material-hash-values/.

[157] Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008, Pub. L. No. 110-401, 122 Stat. 4229.

[158] Kristie Canegallo, *Our Efforts to Fight Child Sexual Abuse Online*, GOOGLE: THE KEYWORD (Feb. 24, 2021), https://blog.google/technology/safety-security/our-efforts-fight-child-sexual-abuse-online/.

[159] *PhotoDNA*, MICROSOFT, https://www.microsoft.com/en-us/photodna; Petter Christian Bjelland et al., *Practical Use of Approximate Hash Based Matching in Digital Investigations*, 11 DIGIT. INVESTIG. 18, 20 (2014) (discussing Microsoft's PhotoDNA as a technology using approximate hash-based matching to measure perceptual similarity in pictures).

[160] United States v. Jacobsen, 466 U.S. 109 (1984).

[161] Walter v. United States, 447 U.S. 649 (1980).

[162] *Jacobsen*, 466 U.S. at 115.

violate the Fourth Amendment because of their private character." [163] According to Justice Stevens, "[o]nce frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now-nonprivate information."[164] In other words, "[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated."[165] That, the Court decided, "must be tested by the degree to which they [the government] exceeded the scope of the private search."[166]

At the core of the private search doctrine is how to test whether the government has exceeded the scope of private search. In *Jacobsen*, DEA officers did not merely gaze at the white powder, as FedEx employees did; rather, they did a field test of the white powder and found it was cocaine, without a search warrant. The *Jacobsen* Court, however, did not consider the field test had exceeded the scope of private search, as "[a] chemical test that merely discloses whether or not a particular substance is cocaine does not compromise any legitimate interest in privacy." [167] This was because the "legitimate interest in privacy" was constrained by the underlying federal statute.

> Congress has decided—and there is no question about its power to do so—to treat the interest in 'privately' possessing cocaine as illegitimate; thus governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest.[168]

In other words, the *Jacobsen* Court considered the field test reasonable under the Fourth Amendment based on the unique character of the technique applied: "[t]he field test at issue could disclose only one fact previously unknown to the agent—whether or not a suspicious white powder was cocaine."[169] The field test "could tell him nothing more, not even whether the substance was sugar or talcum powder."[170] In their dissenting opinion, Justice Brennan and Justice Marshall considered that "the Court adopts a general rule

---

[163] *Id.* at 115.

[164] *Id.* at 117.

[165] *Id.*

[166] *Id.* at 115.

[167] *Id.* at 123.

[168] *Id.*

[169] *Id.* at 122.

[170] Justice Brennan disagreed, stating:

What is most startling about the Court's interpretation of the term 'search,' . . . is its exclusive focus on the nature of the information or item sought and revealed through the use of a surveillance technique, rather than on the context in which the information or item is concealed.).

Id. at 122, 137 (Brennan, J., dissenting).

that a surveillance technique does not constitute a search if it reveals only whether or not an individual possesses contraband." [171] By contrast, in *Walter*,[172] packages mistakenly delivered to a private company were opened by its employees.[173] They found boxes of films with explicit descriptions of their contents and unsuccessfully attempted to view portions of the film before calling the FBI. Without a search warrant, the FBI screened the films on a government projector and found obscene contents.[174] A plurality of the Court found the search implicated the Fourth Amendment.[175] Justice Stevens stated, "[t]he projection of the films was a significant expansion of the search that had been conducted previously by private party and therefore must be characterized as a separate search."[176]

2. Photos in the Cloud

Hash-value matching for files stored in the cloud seemed a perfect factual pattern for the private search doctrine. Internet service providers (ISPs) are not required to monitor or "affirmatively search" their users' files;[177] but "as soon as reasonably possible after obtaining actual knowledge,"[178] they are required to report to NCMEC via its online tool called the CyberTipline.[179] NCMEC, which acts as a clearinghouse, must make each report available to law enforcement. [180] Because ISPs are private companies, [181] NCMEC is considered a government entity or agent.[182] Hash-value matching is a tool

---

[171] *Id.* at 137 (Brennan, J., dissenting).

[172] *Walter*, 447 U.S. 649.

[173] *Id.* at 651–52.

[174] *Id.* at 652.

[175] *Id.*

[176] *Id.* at 657.

[177] 18 U.S.C. § 2258A(f).

[178] *Id.* § 2258A(a)(1)(A).

[179] *Id.* § 2258A(a)(1)(B) (requiring ISPs to provide "the mailing address, telephone number, facsimile number, electronic mailing address of, and individual point of contact for, such provider").

[180] *Id*. § 2258A(c).

[181] United States v. Stevenson, 727 F.3d 826 (8th Cir. 2013) (holding that using hash-value matching tool to discover child pornography in plaintiff's files, AOL, Inc., the Internet service provider, was not a government agent for the purpose of the Fourth Amendment). *See also* United States v. Richardson, 607 F.3d 357 (4th Cir. 2010) (holding that AOL's conduct in scanning emails did not equate to a governmental search that would trigger the Fourth Amendment); United States v. Cameron, 699 F.3d 621 (1st Cir. 2012) (holding that Yahoo did not act as a government agent in searching user's accounts); United States v. Keith, 980 F. Supp. 2d 33 (D. Mass. 2013) (holding that AOL was not an agent of the government by sending a file to NCMEC); United States v. Wolfenbarger, No. 16-CR-00519-LHK-1, 2019 WL 3037590 (N.D. Cal. 2019) (holding that Yahoo did not act as a government agent in hash-value matching search).

[182] United States v. Ackerman, 831 F.3d 1292, 1295–1304 (10th Cir. 2016) (recognizing NCMEC as a government entity or agent in the search).

promising the capability of exclusively detecting child pornography; the private search doctrine seems a natural application.[183]

In *United States v. Reddick*,[184] plaintiff Henry Reddick uploaded digital images to his Microsoft SkyDrive, which used the PhotoDNA program to automatically scan the hash values of user-uploaded files and compare them against the hash values of known images of child pornography. Microsoft sent a report to NCMEC, which forwarded the information to Corpus Christi, Texas Police. Police opened each suspect file and confirmed that each contained child pornography.[185] The Fifth Circuit found the *Jacobsen* principle "readily applies" in this case.[186] Like the field test in *Jacobsen*, the Fifth Circuit reasoned that "opening the file merely confirmed that the flagged file was indeed child pornography, as suspected."[187] Unlike the film screening in *Walter*, according to the Fifth Circuit, "when [police] opened the files, there was no 'significant expansion of the search that had been conducted previously by a private party' sufficient to constitute 'a separate search.'"[188]

Similarly, in *United States v. Miller*,[189] the plaintiff's attached files in his Gmail account had hash values matching images in Google's child pornography repository. Google sent a CyberTip report to NCMEC.[190] No Google employee had viewed the files;[191] it was the police in Kenton County, Kentucky, that opened the files and viewed them.[192] The Sixth Circuit recognized that viewing the images is not the binary test technique that was essential in *Jacobsen* because the police could detect something else.[193] Thus, the Sixth Circuit decided to compare Google's search of the images with FedEx's search of the boxes in *Jacobsen*.[194] Relying on the trial court's finding that Google's search was sufficiently reliable and that the plaintiff did not question it, the Sixth Circuit concluded that under *Jacobsen*, the private search doctrine would allow police to reexamine the images "more thoroughly."[195]

---

[183] United States v. Bonds, No. 5:21-CR-00043-KDB-DCK, 2021 WL 4782270, (W.D. N.C. Oct. 13, 2021); United States v. Wilson, 13 F.4th 961 (9th Cir. 2021), United States v. Miller, 982 F.3d 412 (6th Cir. 2020), United States v. Reddick, 900 F.3d 636 (5th Cir. 2018).

[184] *Reddick*, 900 F.3d at 637–38.

[185] *Id.* at 638.

[186] *Id.* at 639.

[187] *Id.*

[188] *Id.*

[189] *Miller*, 982 F.3d at 420.

[190] *Id.*

[191] *Id.*

[192] *Id.*

[193] *Id.* at 429.

[194] *Id.*

[195] *Id.* at 431.

Despite their slightly different approaches, the Fifth and Sixth Circuits share a common interpretation of *Jacobsen*. However, the Tenth and Ninth Circuits adopt a narrower reading of *Jacobsen*. In *United States v. Ackerman*, AOL used its Image Detection and Filtering Process (IDFP), an automated program to detect hash-value matches with child pornography in plaintiff Walter Ackerman's email.[196] AOL sent a report to NCMEC, which included Ackerman's email and four attached images.[197] An NCMEC analyst opened the email and viewed each of the attached images.[198] In the opinion written by then Judge Gorsuch, the Tenth Circuit concluded that the private search doctrine did not apply.[199] For Judge Gorsuch, the opening of the email and the viewing of the attached images were "pretty obviously a 'search.'"[200] This was because "AOL never opened the email itself. Only NCMEC did that, and in at least this way exceeded rather than repeated AOL's private search."[201] Judge Gorsuch compared the email to a container; "when NCMEC opened Mr. Ackerman's email it could have learned any number of private and protected facts, for (again) no one before us disputes that an email is a virtual container, capable of storing all sorts of private and personal details. . . ."[202] Furthermore, "this particular container *did* contain three additional attachments, the content of which AOL and NCMEC knew nothing about before NCMEC opened them too."[203] For these reasons, Judge Gorsuch considered the reasoning in *Walter* to control here.[204]

Judge Gorsuch also offered an alternative approach to the same question by the notion of trespass announced in *United States v. Jones*.[205] "Reexamining the facts of *Jacobsen* in light of *Jones*, it seems at least possible the Court today would find that a 'search' did take place there."[206] This is because the *Jacobsen* field test constituted trespass to chattels.[207] Thus, for Judge Gorsuch, *Jones* leaves an uncertain status for *Jacobsen*.[208] Regardless, the Tenth Circuit

---

[196] United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016).

[197] *Id.* at 1294.

[198] *Id.*

[199] *Id.*

[200] *Id.* at 1304.

[201] *Id.* at 1306.

[202] *Id.*

[203] *Id.*

[204] *Id.*

[205] *Id.* at 1307 (citing United States v. Jones, 565 U.S. 400 (2012)).

[206] *Id.*

[207] *Id.*

[208] *Id.* ("Given the uncertain status of *Jacobsen* after *Jones*, we cannot see how we might ignore *Jones*'s potential impact on our case.").

concluded that the private search doctrine did not apply. The case was remanded back to the trial court.[209]

More recently, the Ninth Circuit joined the Tenth Circuit in having a more skeptical view of the *Jacobsen* interpretation. In *United States v. Wilson*,[210] Google reported to NCMEC after detecting hash-value matches in Luke Wilson's email after he uploaded four images to his email account. No one at Google had opened or viewed Wilson's email attachments. Someone at NCMEC then, without opening or viewing the attachments, sent them to the San Diego Internet Crimes Against Children Task Force, where an officer viewed the email attachments without a warrant. The Ninth Circuit ruled that the private search exception to the Fourth Amendment did not apply. Like the Tenth Circuit in *Ackerman*, the Ninth Circuit considered that the *Walter* principle controlled the case, as "[v]iewing Wilson's email attachments—like viewing the movie in *Walter*—substantively expanded the information available to law enforcement far beyond what the label alone conveyed, and was used to provide probable cause to search further and to prosecute."[211] Thus, the police exceeded the scope of Google's private search.[212]

Federal courts have transformed the private search doctrine of *Jacobsen* and *Walter* to cyberspace. Despite their differences in reading and interpreting the Supreme Court decisions, none of the courts considered that the private searches in both *Jacobsen* and *Walter* were accidental, not systemic and constant, as hash-value matching is in cyberspace. In cyberspace, private search by hash-value matching is neither accidental, nor limited by time or space.

III. DATA AS PERSONAL RIGHTS: THE EUROPEAN UNION

The notion of privacy in the European context was premised on the "rights of personality" (*Persönlichkeitsrecht*) envisioned by German private law jurists,[213] and a similar notion in *les droits de la personnalité* developed by French jurists.[214] In France, without the benefit of a privacy clause in the Civil

---

[209] United States v. Ackerman, 296 F.Supp.3d 1267 (D. Kan. 2017), *aff'd on appeal*, 804 Fed. App'x. 900 (10th Cir. 2020), *cert. denied*, 141 S.Ct. 458 (2020).

[210] United States v. Wilson, 13 F.4th 961 (9th Cir. 2021).

[211] *Id.* at 973.

[212] *Id.*

[213] These private law jurists include Karl Gareis, Otto Gierke and Joseph Kohler, *see Protection of Personality Rights in the Law of Delict/Torts in Europe: Mapping out Paradigms*, *in* PERSONALITY RIGHTS IN EUROPEAN TORT LAW 5 (Gert Brüggemeier et. al. eds., 2010); HUW BEVERLY-SMITH ET. AL., PRIVACY, PROPERTY AND PERSONALITY: CIVIL LAW PERSPECTIVES ON COMMERCIAL APPRIORIATION (2005); Stig Strömholm, *Right of Privacy and Rights of the Personality: A Comparative Survey* (Int'l Comm'n Jurists, Working Paper, 1967).

[214] Étienne Picard, *The Right to Privacy in French Law*, *in* PROTECTING PRIVACY 49 (Basil S. Markesinis ed. 1999); Wenceslas J. Wagner, *The Development of the Theory of the Right to Privacy in France*, 1971 WASH. U. L. Q. 45 (1971).

Code, the French courts had developed legal doctrines to protect name and likeness since the mid of the nineteenth-century.[215] German private law jurists were careful to distinguish personality rights from property. Karl Gareis, private law professor from Munich, reiterated that "[r]ights of personality are related to property without depending exclusively on proprietary ends, and without being protected essentially for the sake of property."[216] In 1889, Otto von Gierke, a professor at Berlin University known for his critique of the German Civil Code, emphasized, "[a]ll property exists merely for the sake of the person, and surrounding every proprietary relationship is the right of developing one's personality." [217] The Continental personality theory was consistent with claims of Judge Cooley, and those of Warren and Brandeis; it may have inspired Dean Roscoe Pound in his support of Warren and Brandeis in the debate in America.[218]

Personality right theory itself was not enough, as history shows. [219] However, after World War II, institutions developed to provide increasing guarantee. This was first achieved by the European Court of Human Rights in the 1980s and 1990s. In the era of the internet and social media, the Court of Justice of the European Union undertook the functions of the constitutional court as guardian of the constitutional norms.[220]

---

[215] Jeanne M. Hauch, *Protecting Private Facts in France: The Warren and Brandeis Tort Is Alive and Well and Flourishing in Paris*, 68 TUL. L. REV. 1219 (1994); Wenceslas J. Wagner, *The Right to One's Own Likeness in French Law*, 46 IND. L.J. 1, 5 (1970); W. J. Wagner, *Photography and the Right to Privacy: The French and American Approaches*, 25 CATH. LAW. 195 (1980); HUW BEVERLEY-SMITH et al., *supra* note 213.

[216] KARL GAREIS, INTRODUCTION TO THE SCIENCE OF LAW, 1911: SYSTEMATIC SURVEY OF THE LAW AND PRINCIPLES OF LEGAL STUDY 123 (Albert Kocourek trans., 1911) (3rd ed. 1905).

[217] Otto von Gierke, *The Social Role of Private Law* (Ewan McGaughey trans.), 19 GERMAN L.J. 1017, 1092 (2018).

[218] *Supra* note 43. In his articles on personality in 1916 and 1915, Pound repeated, acknowledged and cited Karl Gareis, Otto Gierke, among others. The influence by Continental European jurists on Pound was well documented. *See* William L. Grossman, *The Legal Philosophy of Roscoe Pound*, 44 YALE L.J. 605 (1935) (the influence of Ihering and Kohler); DAVID WIGDOR, ROSCOE POUND: PHILOSOPHER OF LAW (1974); DAVID M. RABBAN, LAW'S HISTORY: AMERICAN LEGAL THOUGHT AND THE TRANSATLANTIC TURN TO HISTORY 423 (2013).

[219] ALEXANDER SOMEK, *Authoritarian Constitutionalism: Austrian Constitutional Doctrine 1933 to 1938 and Its Legacy*, *in* DARKER LEGACIES OF LAW IN EUROPE: THE SHADOW OF NATIONAL SOCIALISM AND FASCISM OVER EUROPE AND ITS LEGAL TRADITIONS 361 (Christian Joerges & Navraj Singh Ghaleigh eds., 2003).

[220] Georg Schmitz, *The Constitutional Court of the Republic of Austria 1918–1920*, 16 RATIO JURIS 240 (2003); Sara Lagi, *Hans Kelsen and the Austrian Constitutional Court (1918–1929)*, 9 COHERENCIA 273 (2012); THE GUARDIAN OF THE CONSTITUTION: HANS KELSEN AND CARL SCHMITT ON THE LIMITS OF CONSTITUTIONAL LAW (Lars Vinx ed., 2015).

A. European Court of Human Rights: 1980s

The European Human Rights Convention was signed in 1950 based on painful lessons learned from the Nazi experience in Europe.[221] Article 8, when it was first proposed,[222] followed Article 12 of the Universal Declaration of Human Rights.[223] The European Court of Human Rights was established in 1959.[224] After its initial dormant years, the Court emerged after 1975 as a powerful driving force for European integration.[225] This supernational judicial body functioned as a constitutional court to establish standards for its member states.[226]

1. The British Experience

The first telephone tapping case in the United Kingdom was brought to the English High Court's Chancery Division in *Malone v. Metropolitan Police*

---

[221] ED BATES, THE EVOLUTION OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS: FROM ITS INCEPTION TO THE CREATION OF A PERMANENT COURT OF HUMAN RIGHTS 44–107 (2010) (describing the drafting process of the European Convention) [hereinafter BATES, THE EVOLUTION]; *see also* Mark Mazower, *The Strange Triumph of Human Rights, 1933–1950*, 47 HIST. J. 379 (2004) (on the broader background of human rights discourse).

[222] *Proposals by Mr. P. H. Teitgen*, Rapporteur (Doc. A 116) (Aug. 29, 1949), *in* OF THE 'TRAVAUX PREPARATOIRES' OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 166, 168 (1975) (Preparatory Commission of the Council of Europe, Committee of Ministers, Consultative Assembly 11 May–13 July 1949). This proposed language became Article 12 in its September 5, 1949 draft of the Convention: "No one shall be subjected to arbitrary interference with his privacy, family, and home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." *Id.* at 192, 196.

[223] G.A. Res. 217A (III), Universal Declaration of Human Rights, (Dec. 10, 1948) ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation."). For the drafting process of this clause between 1947 and 1948, see Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14 HUM. RTS. L. REV. 441 (2014). It is likely that Article 12 originated from Article 6 of Sir Hersch Lauterpacht's "International Bill of the Rights of Man," which provided that, "[t]he sanctity of the home and the secrecy of correspondence shall be respected." SIR HERSCH LAUTERPACHT, AN INTERNATIONAL BILL OF THE RIGHTS OF MAN 70 (1945). On Lauterpacht, see A. W. Brian Simpson, *Hersch Lauterpacht and the Genesis of the Age of Human Rights*, 120 L. Q. REV. 49 (2004); *see also* BATES, THE EVOLUTION, *supra* note 221, at 35 ("had a significant influence on the first proposals for a European Convention [on Human Rights].").

[224] BATES, THE EVOLUTION, *supra* note 221, at 124–33.

[225] *Id.* at 142 (noting that the number of cases brought to the Court and the number of judgments issued by the Court have significantly increased from 1975).

[226] Many of the comments by Jochen Abraham Frowein, a member of the European Commission for Human Rights from 1973 to 1993 and Vice-President from 1981 to 1993, reflected this perspective. *See* Jochen A. Frowein, *European Integration through Fundamental Rights*, 18 U. MICH. J.L. REFORM 5 (1984); Jochen A. Frowein, *Experiences with the European Convention on Human Rights*, 5 S. AFR. J. ON HUM. RTS. 196 (1989); Jochen A. Frowein, *The Transformation of Constitutional Law through the European Convention on Human Rights*, 41 ISR. L. REV. 489 (2008). *See,* also, JUKKA VILJANEN, THE EUROPEAN COURT OF HUMAN RIGHTS AS A DEVELOPER OF THE GENERAL DOCTRINES OF HUMAN RIGHTS LAW: A STUDY OF THE LIMITATION CLAUSES OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS (2003).

Commissioner (1979).[227] In this case, plaintiff James Malone, an antique dealer, was charged with offenses relating to stolen property.[228] During the trial, the prosecution admitted there was an interception of Malone's telephone line. Post Office officials conducted the wiretaps and made the recordings available to police for transcription and use.[229] Malone contended that tapping was unlawful in English law. To this question, however, the presiding judge, Vice-Chancellor Sir Robert Megarry, could not find any violation of English law.[230] The court ruled that plaintiff's claim failed in its entirety.[231] The core of the judge's ruling was that "tapping" and obtaining the information were separate acts: on the one hand, the police did not do anything wrong because all they did was "ask for information and received it when obtained."[232] While the court recognized that "[a]ll the work of tapping was done by the Post Office,"[233] that cannot be trespass, the judge reasoned, because "all that is done is done within the Post Office's own domain."[234] Nor was it an offense because it was information "obtained by a Crown servant in the course of his duty or under the authority of the Postmaster General . . ."[235]

After the English High Court's decision, James Malone brought his case to the European Court of Human Rights (ECtHR), alleging a violation of Article 8 of the European Convention of Human Rights (ECHR).[236] Article 8 of the Convention protects "the right to respect for his private and family life," and that any interference with such privacy right must be "in accordance with the law" and "necessary in a democratic society."[237] The Court ruled in August

---

[227] Malone v. Metropolitan Police Commissioner (No.2) [1979] Ch. 344 (Eng.).

[228] *Id.* at 349.

[229] *Id.* at 344, 355.

[230] *Id.* at 356 ("There was no English authority that in any way directly born on the point.").

[231] *Id.* at 383.

[232] *Id.* at 368.

[233] *Id.*

[234] *Id.* at 369.

[235] *Id.* at 378. The Vice-Chancellor's judicial opinion closely followed the Birkett Report, which was the result of the 1957 parliamentary inquiry into the "state of law" on telephone interceptions. The Committee was chaired by Norman Birkett, so the Report is better known as the Birkett Report. *See*, PRIVY COUNCILORS APPOINTED TO INQUIRE INTO THE INTERCEPTION OF COMMUNICATIONS COMMITTEE, REPORT, 1957 HC 31 (UK).

[236] Malone v. United Kingdom, App. No. 8691/79, Eur. Ct. H.R. 10 (Aug. 2, 1984), ¶ 1.

[237] The United Kingdom was one of the initial signatory countries in 1950 of The Convention for the Protection of Human Rights and Fundamental Freedoms, better known as the European Convention on Human Rights. Article 8 of the Convention provides:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence; (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the

1984 against the United Kingdom.[238] The Court had no trouble recognizing that "telephone conversations are covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8."[239] The Court had decided on that issue a few years earlier in *Klass v. Germany*,[240] where it was asked to examine the controversial surveillance law in West Germany.[241] The Court made a powerful statement regarding privacy under Article 8: "[W]here a State institutes secret surveillance the existence of which remains unknown to the persons being controlled, with the effect that the surveillance remains unchallengeable, Article 8 (art. 8) could to a large extent be reduced to a nullity."[242]

Rather, the focus in *Malone* was on the second prong—the legal bases.[243] Here, the Court found interception of communications constituted an interference with Malone's Article 8 rights and was not "in accordance with the law."[244] The Court reiterated that "the phrase 'in accordance with the law' does not merely refer back to domestic law but also relates to the quality of the law."[245] In other words, "[T]here must be a measure of legal protection in domestic law against arbitrary interferences by public authorities . . . . Especially where a power of the executive is exercised in secret, the risks of arbitrariness are evident."[246]

The external constitutional constraint by the European Court of Human Rights thus changed the course on the issue of wiretapping in Great Britain.

2. The French Experience

The French experience was similar. In France, the Civil Code did not incorporate Article 9, the right to privacy, until 1970.[247] France ratified the

---

prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S.

[238] *Malone*, *supra* note 227 ¶ 1.

[239] *Id.* ¶ 64.

[240] Klass v. Germany, App. No. 5029/71 (Sept. 6, 1978), https://hudoc.echr.coe.int/fre?i=001-57510. *See also* James G. Carr, *Wiretapping in West Germany*, 29 AM. J. COMP. L. 607 (1981).

[241] *See* Note, *Recent Emergency Legislation in West Germany*, 82 HARV. L. REV. 1704 (1969). (noting the amendment of StPO, together with GG Article 10, was part of the "emergency legislation" in the broader amendment of the Basic Law in 1968).

[242] *Klass*, 5029/71 ¶ 36.

[243] *Malone*, 8691/79 ¶ 65.

[244] *Id.* ¶ 80.

[245] *Id.* ¶ 67.

[246] *Id.* ¶ 67.

[247] *See* CODE CIVIL [C. CIV.] [CIVIL CODE] art. 9 (Fr.) (1970) ("Everyone has the right to respect for his private life."). *See also* Picard, *supra* note 214.

European Human Rights Convention in March 1974.[248] The European Court of Human Rights fundamentally shaped the law in France through its rulings on telephone tapping in *Kruslin v. France* and *Huvig v. France.*[249] The *Kruslin* case was similar to *Malone*. Jean Kruslin was charged with murder based on recordings of phone conversations. The police had obtained a warrant from an investigating judge to tap the telephone of another suspect in a murder case, and it happened that Kruslin was staying with him.[250] When the police learned of the conversation between Kruslin and his partner in another murder case, Kruslin was arrested and charged with murder.[251] Kruslin appealed to the Court of Cassation, but was not successful. At the European Court of Human Rights, Kruslin contended that French law violated his right under Article 8.[252] Like the *Malone* case, the Court had no difficulty applying prong one in recognizing interference with private life; the contention was focused on the second prong of Article 8.[253] While the Court conceded "in accordance with the law," it further focused on "the quality of law," an interpretation of the second prong in the *Malone* case.[254] The Court went further when it made the statement:

> Tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated.[255]

By measuring this standard, the Court found that the French law failed to deliver that: "French law, written and unwritten, does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities."[256] The *Kruslin* ruling pushed the French Parliament to pass the 1991 Wiretapping Act,[257] the first legal framework on

---

[248] BATES, THE EVOLUTION, *supra* note 221.

[249] Kruslin v. France, App. No. 11801/85 (Apr. 24, 1990), https://hudoc.echr.coe.int/eng?i=001-57626; Huvig v. France, App. No. 11105/84 (Apr. 24, 1990), https://hudoc.echr.coe.int/eng?i=001-57627.

[250] *Kruslin*, App. No. 11801/85 ¶ 9.

[251] *Id.* ¶ 10.

[252] *Id.* ¶ 23.

[253] *Id.* ¶ 26.

[254] *Id.* ¶ 33.

[255] *Id.*

[256] *Id.* ¶ 36.

[257] Loi 91–646 du 10 juillet 1991 relative au secret des correspondences émises par la voie des communications électroniques [Law 91–646 of July 10, 1991 Concerning the Secrecy of Correspondences Transmitted Through Electronic Communications], JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], July 13, 1991.

wiretapping in French history. Professor Edward A. Tomlinson observed, "[t]he French criminal courts and Parliaments acted to restrict wiretapping only because of external pressures from France's new Constitutional Council and Europe's new Court of Human Rights."[258]

From the rulings in *Klass*, *Malone,* and *Kruslin*, it is clear that the European Court of Human Rights did not try to work on the textual meaning of "private life" or the treaty-making history for the meaning of privacy.[259] It simply adopted a broad notion of privacy and thus often had no difficulty on the first prong of Article 8. This basic reading of Article 8 strategically shifted the focus to the second prong, "in accordance with domestic law" and "necessary in a democratic society."[260] This shift made the Court's primary function as a constitutional guardian of fundamental rights in Europe.

3. Third-party Data

Similarly, in *Funke v. France* (1993), French customs officers came to Jean-Gustave Funke's house, asking him to produce financial records from foreign banks for the past three years. [261] They also, without judicial authorization, searched his house and seized documents.[262] The Court found the search and seizure breached the second prong of Article 8 of the Convention for lack of procedural safeguards to prevent abuse.[263] Further, In *A. v. France* (1993),[264] Mrs. A., a French national, was charged with attempted murder based on the recording of a phone conversation between her and an informant who volunteered the phone call. The French government contended that the intercepted conversation was a deliberate preparation of a criminal nature, and thus fell outside the scope of private life.[265] The European Commission contended that a telephone conversation did not lose its private character simply because its content concerned or might concern the public interest.[266] The Court did not comment on the Commission's view; rather, it focused on the nature of the scheme as an interference of public authority:

---

[258] Edward A. Tomlinson, *The Saga of Wiretapping in France: What It Tells Us about the French Criminal Justice System*, 53 LA. L. REV. 1091, 1094 (1993).

[259] This led to concerns for some commentators. *See* A. M. Connelly, *Problems of Interpretation of Article 8 of the European Convention on Human Rights*, 35 INT'L & COMP. L.Q. 567 (1986).

[260] Convention for the Protection of Human Rights and Fundamental Freedoms, *supra* note 237.

[261] Funke v. France, App. No. 10828/84, (Feb. 25, 1993), https://hudoc.echr.coe.int/eng?i=001-57809.

[262] *Id.* ¶ 7.

[263] *Id.* ¶ 59.

[264] A. v. France, App. No. 14838/89 (Nov. 23,1993), https://hudoc.echr.coe.int/eng?i=001-57848.

[265] *Id.* ¶ 34.

[266] *Id.* ¶ 35.

> The [police officer] played a decisive role in conceiving and putting into effect the plan to make the recording, by going to see the Chief Superintendent and then telephoning Mrs. A. [The officer], for his part, was an official of a "public authority". He made a crucial contribution to executing the scheme by making available for a short time his office, his telephone and his tape recorder.[267]

From the nature of this scheme, the Court reasoned that "the public authorities were involved to such an extent that the State's responsibility under the Convention was engaged."[268] It is obvious, from this reasoning, that the Court agreed with the Commission's argument and took it for granted.

Is conversation over an office phone protected by Article 8? In *Halford v. United Kingdom* (1997),[269] Alison Halford, a British police officer, alleged that her office telephone was intercepted,[270] violating Article 8. As mentioned earlier, shortly after the *Malone* ruling, Great Britain enacted the Interception of Communications Act 1985.[271] But the 1985 Act only covered public telephone networks. However, Halford's office phones were part of the police's internal telephone network, not a public network.[272] The British government contended that telephone calls from Halford's workplace fell outside the protection of Article 8 because she had no reasonable expectation of privacy in them.[273] The Court was not convinced.[274] The Court noted that there was no evidence of any warning given to Halford about interception.[275] The Court found other factors reinforced Halford's expectation of privacy:

> As Assistant Chief Constable she had sole use of her office where there were two telephones, one of which was specifically designated for her private use. Furthermore, she had been given the assurance, in response to a memorandum, that she

---

[267] *Id.* ¶ 36.

[268] *Id.*

[269] Halford v. United Kingdom, App. No. 20605/92, Eur. Ct. H.R. 1004 (Jun. 25, 1997). https://hudoc.echr.coe.int/eng?i=001-58039. Samantha Besson, *The Reception in Ireland and the United Kingdom*, *in* A EUROPE OF RIGHTS: THE IMPACT OF THE ECHR ON NATIONAL LEGAL SYSTEMS 31–106 (Helen Keller & Alec Stone Sweet eds., 2008).

[270] *Id.* ¶ 12.

[271] Interception of Communications Act 1985, c. 56 (UK).

[272] Halford, App. No. 20605/92 ¶ 36 ("The 1985 Act does not apply to telecommunications systems outside the public network, such as the internal system at Merseyside police headquarters, and there is no other legislation to regulate the interception of communications on such systems.").

[273] *Id.* ¶ 43.

[274] *Id.* ¶ 46.

[275] *Id.* ¶ 45.

> could use her office telephones for the purposes of her sex-discrimination case . . .[276]

In *Lambert v. France* (1998),[277] Lambert was charged with unlawful possession of weapons based on evidence collected from tapping the telephone line of a third party.[278] In domestic proceedings, the Court of Cassation ruled that Lambert had no standing (*locus standi*) because it was a third party's telephone line that was intercepted.[279] The European Court of Human Rights disagreed. It commented that "it is of little importance that the telephone tapping in question was carried out on the line of a third party."[280] Similarly, in *Kopp v. Switzerland*,[281] the European Court of Human Rights did not find third party status a reason to look away. Here, Hans Kopp was a lawyer in Zurich.[282] Police had Kopp's law firm's telephone lines tapped though he was not a suspect but only a third party in a criminal investigation.[283] The Swiss government contended that tapping was not "interference" in law because none of the recorded conversations had been brought to the knowledge of the prosecuting authorities, all the recordings had been destroyed, and no use whatsoever had been made of them.[284] The Court ruled "[t]he subsequent use of the recordings made has no bearing" on the finding that it was an "interference."[285]

In sum, during the 1980s and 1990s, the European Court of Human Rights played the role of a powerful constitutional court in safeguarding privacy rights through its interpretation of Article 8 of the European Convention. Through its rulings, the Court forcefully brought wiretapping under the constitutional framework in Europe. Privacy, understood and interpreted by the Court, was more a personal right that attached to the person, rather than defined by property. What Karl Gareis and Otto von Gierke had imagined finally became true one hundred years later.

---

[276] *Id.*

[277] Lambert v. France, App. No. 88/1997/872/1084 (Aug. 24, 1998), https://hudoc.echr.coe.int/eng?i=001-58219.

[278] *Id.* ¶¶ 8–10.

[279] *Id.* ¶ 14.

[280] *Id.* ¶ 21.

[281] Kopp v. Switzerland, App. No. 13/1997/797/1000 (Mar. 25, 1998), https://hudoc.echr.coe.int/eng?i=001-58144.

[282] *Id.* ¶ 6.

[283] *Id.* ¶ 16.

[284] *Id.* ¶ 51.

[285] *Id.* ¶ 53.

B. The 2006 Data Retention Directive

In the aftermath of September 11 and arrival of the internet, however, members of the European Union faced the same pressure to seek data for surveillance purposes as in the United States.[286] After the September 11 attacks in the United States, terrorist attacks happened in Madrid (March 11, 2004), London (July 7, 2005), Oslo (July 22, 2011), and Paris (November 13, 2015); concerns of terrorism are one of the main driving forces for facilitating surveillance in Europe.[287] One key area of facilitating surveillance is data retention. France enacted in November 2001 a statute on public safety, Law no. 2001-1062, [288] which required the collection and retention of telecommunications traffic data. In Great Britain, the Anti-terrorism, Crime and Security Act 2001 was enacted three months after September 11,[289] granting the Secretary of State the power to proscribe rules on data retention by service providers. [290] In August 2003, Austria passed the Telecommunications Act of 2003 (Telekommunikationsgesetz, or TGK).[291] Article 102a contained broad requirements for data retention. Even in liberal Sweden, the Electronic Communications Act was passed in July 2003.[292] Chapter 6 Section 22.1 made it an obligation for service providers to share data with law enforcement.[293] However, the supranational court—the Court of Justice of the European Union (CJEU)— provided constitutional constraints on member countries, limiting their ability to extract data from service providers.

The measures to access data by private service providers, however, were contrary to EU law at the time. Article 6 of the Personal Data Directive (Directive 95/46/EC) prohibited the storage of data beyond the duration

---

[286] THOMAS MATHIESEN, TOWARDS A SURVEILLANT SOCIETY: THE RISE OF SURVEILLANCE SYSTEMS IN EUROPE (2013).

[287] *Id.* at 62 (arguing that Europe's surveillance systems "are to a large extent, or even primarily, geared towards . . . three enemy images." These three "enemy images" are: terrorism, organized crimes, and foreigners at the borders).

[288] Loi 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne [Law 2001-1062 of Nov. 15, 2001 on Daily Safety], J. OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], July 3, 2001, p.18215; Winston Maxwell, *Systematic Government Access to Private-Sector Data in France*, 4 INT'L DATA PRIV. L. 4 (2014).

[289] Anti-terrorism, Crime and Security Act, (2001) c. 24 (UK), https://www.legislation.gov.uk/ukpga/2001/24/contents.

[290] *Id.* § 102; Clive Walker & Yaman Akdeniz, *Anti-Terrorism Laws and Data Retention: War Is Over*, 54 N. IR. LEGAL Q. 159 (2003) (critiquing the Act).

[291] TELEKOMMUNIKATIONSGESETZ [TKG] [TELECOMMUNICATIONS ACT] BUNDESGESETZBLATT No. 70/2003 (Austria); Andreas Lehner, *Data Retention: A Violation of the Right to Data Protection, Constitutional Developments in Austria*, 8 VIENNA J. INT'L CONST. L. 445 (2014) (discussing Article 102's impact on data retention).

[292] LAG OM ELEKTRONISK KOMMUNIKATION (Svensk författningssamling [SFS] 2003:389) (Swed).

[293] *Id.*

required to fulfill the purposes of data collection.[294] In December 1997, the EU Parliament passed Directive 97,[295] which specifically required that "[t]raffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available tele-communications service must be erased or made anonymous upon termination of the call . . ."[296] In the years immediately after the September 11 attacks, the European Parliament passed Directive 2002/58,[297] which specifically required:

> Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so in accordance with Article 15(1).[298]

However, on April 28, 2004, France, Ireland, Sweden, and Great Britain submitted a proposal to the Council of the European Union to change this.[299] The terrorist bombings in London in July 2005 gave Great Britain, which happened to inhabit the presidency of the Council, both conviction and moral leadership to push for an agreement on data retention. Great Britain achieved

---

[294] Directive 95/46/EC, art. 6, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281) 1, 40; *see* Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431 (1995) (stating that the negotiation for the Directive dates back to the 1980s); Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 448 (1995) (explaining "[T]he commitment to fundamental rights forces the Commission to achieve not merely some level of protection, but protection of 'a high degree,' which in the Union's language means the maximum possible").

[295] Directive 97/66/EC, European Parliament and of the Council of 15 December 1997 Concerning the Processing of Personal Data and on the Protection of Privacy in the Telecommunications Sector, 1997 O.J. (L 24) 1.

[296] *Id.* art. 6(1).

[297] Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002, Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector), 2002 O.J. (L 201) 37, *amended by* Directive 2009/136/EC of the European Parliament and of the Council of Nov. 25, 2009, 2009 O.J. (L 337) 11 [hereinafter, "Directive 2002/58"].

[298] *Id.* art. 5(1).

[299] *See* Council Document 8958/04, Draft Framework Decision on the Retention of Data Processed and Stored in Connection with the Provision of Publicly Available Electronic Communications Services or Data on Public Communications Networks for the Purpose of Prevention, Investigation, Detection and Prosecution of Crime and Criminal Offences Including Terrorism (Apr. 28, 2004).

this agreement in December 2005. [300] On March 15, 2006, the European Parliament and the Council of the EU passed the Data Retention Directive (Directive 2006/24). [301] Directive 2006/24 made it an obligation for member states to adopt measures "to ensure that the data specified in . . . this Directive are retained in accordance with the provisions thereof."[302] Thus, the 2006 Data Retention Directive reversed the policy established before September 11, making the EU closer to the symbiotic model of the surveillance state.

C. Digital Rights Ireland (2014)

The 2006 Data Retention Directive was widely condemned for disregarding privacy and human rights. [303] However, member states remained under pressure to comply. Ireland and the Slovak Republic challenged the legal basis of the Directive 2006/24 on procedural grounds in 2009, but the challenge was dismissed by the Court of Justice of the European Union (CJEU). [304] On December 21, 2007, Articles 113a and 113b of the German Federal Telecommunications Act (Telekommunikationsgesetz) and the Federal Code of Criminal Procedure were enacted to implement the Directive 2006/24. However, the constitutionality of the statutes came into question. On December 31, 2007, the Working Group on Data Retention, a newly formed privacy advocacy group, filed a formal constitutional complaint with an unprecedented 34,000 individual complainants. On March 10, 2010, the German Constitutional Court (BVerfG) ruled that implementation of the statutes was null and void for violating the German Basic Law Article 10. [305]

---

[300] PROSPECTS FOR THE EUROPEAN UNION IN 2006 AND RETROSPECTIVE OF THE UK'S PRESIDENCY OF THE EU, 1 JULY TO 31 DECEMBER 2005 (Presented to Parliament by the Secretary of State for Foreign and Commonwealth Affairs), 2006, Cm. 6735 (UK).

[301] Directive 2006/24/EC of the European Parliament and of the Council of March 15, 2006, on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54.

[302] *Id.* art. 3(1).

[303] Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 CHI. J. INT'L L. 233 (2007); Patrick Breyer, *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, 11 EUR. L.J. 365 (2005); Stephen McGarvey, *The 2006 EC Data Retention Directive: A Systematic Failure*, 10 HIBERNIAN L.J. 119 (2011); Chris Jones & Ben Hayes, The EU Data Retention Directive: A Case Study in the Legitimacy and Effectiveness of EU Counter-terrorism Policy 6 (Research Paper for the SECILE—Securing Europe through Counter-Terrorism: Impact, Legitimacy and Effectiveness) (2000).

[304] Case C-301/06, Ireland v. Eur. Parl. & Council of the Eur. Union, 2009 E.C.R. I-00593. Ireland had enacted its data retention law similar to those in Great Britain and France. *See* Criminal Justice (Terrorist Offences) Act of 2005 (Act No. 2/2005) (Ir.), http://www.irishstatutebook.ie/eli/2005/act/2/enacted/en/html.

[305] BVerfGE, 1 BvR 256/08, Mar. 2, 2010, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html. For FCC's Press Release No. 11/2010, see "Data Retention in its Present

The Court's ruling was a significant development, but not the first national court challenging Directive 2006/24. Courts in Bulgaria, Cyprus, and Romania ruled against Directive 2006/24 before the German decision; the Czech Republic, Austria, Slovakia, Slovenia, and Hungary did so afterward.[306]

In an unprecedented ruling on April 8, 2014 in *Digital Rights Ireland*,[307] the CJEU held that Directive 2006/24 was invalid. Specifically, the CJEU found the data retention obligation constituted "in itself an interference with the rights guaranteed by Article 7 of the Charter."[308] Similarly, access to the data by the competent national authorities also constituted an interference with the rights guaranteed by Article 7 of the Charter.[309] For such interference with fundamental rights, the Court further found that it did not pass the proportionality test, which required that acts of the EU institutions be appropriate for attaining legitimate objectives and not exceed the limits of what is appropriate and necessary to achieve those objectives.[310] The Court explained that it was troubled by three aspects of Directive 2006/24: first, there were no limits on data—it covered all people and all communication data;[311] second, there were no limits on access—no criteria on national authorities or on their access and use of data;[312] and third, there were no limits on the data retention period—no distinction of different categories of data.[313]

By exercising its judicial review power under the EU constitutional norms, the CJEU redirected the debates on data retention. The decision in *Digital Rights Ireland* (2014) was widely considered a major victory for privacy rights

Form Is Unconstitutional," *available at* https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2010/bvg10-011.html] (last visited July 31, 2021). For commentaries, see Anna-Bettina Kaiser, *German Federal Constitutional Court: German Data Retention Provisions Unconstitutional in Their Present Form: Decision of 2 March 2010*, 6 EUR. CONST. L. REV. 503 (2010); Christian DeSimmone, *Pitting Karlsruhe against Luxembourg—German Data Protection and the Contested Implementation of the EU Data Retention Directive*, 11 GER. L.J. 291 (2010); Hendrik Wieduwilt, *The German Federal Constitutional Court Puts the Data Retention Directive on Hold*, 53 GER Y.B. INT'L L. 917 (2010).

[306] MAREK ZUBIK ET AL., EUROPEAN CONSTITUTIONAL COURTS TOWARDS DATA RETENTION LAWS (2020); *see also* Eleni Kosta, *The Way to Luxemburg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection*, 10 SCRIPTED 339 (2013).

[307] Joined Cases C-293/12 & C-594/12, Digit. Rights Ir. v. Minister for Commc'ns, Marine and Natural Resources and Others, ECLI:EU:C:2014:238 (Apr. 8, 2014).

[308] *Id.* ¶ 34.

[309] *Id.* ¶ 35.

[310] *Id.*¶ 46.

[311] *Id.* ¶¶ 57–59.

[312] *Id.* ¶¶ 60, 61.

[313] *Id.* ¶¶ 63, 64.

and human rights.[314] As a result of the ruling, Directive 2002/58 became the main legal framework of data retention on the EU constitutional level. However, Directive 2002/58 is general and abstract. The CJEU sets itself a task of working out more guidance from the text of Directive 2002/58 by following the constitutional principles of the EU.

D. Constitutional Principles Prevail

Issues soon emerged from Sweden and Great Britain, in the case of *Tele2*. [315] In Sweden, Tele2 Sverige, an electronic communication service provider, immediately after the CJEU's ruling in *Digital Rights Ireland*, informed the Swedish regulator PTS (Post-och telestyrelsen, the Swedish Post and Telecom Authority) that it would cease to retain electronic communications data from April 14, 2014. The Swedish national police authority pressed the PTS, which ordered Tele2 Sverige to retain and share data with the police, based on national legislation. They fought in Swedish courts over the interpretation of EU law, particularly Article 15(1) of Directive 2002/58. Article 15(1)[316] from its text recognizes an exception to the general rule on data protection for national security and fighting crimes.

The Grand Chamber of the CJEU in *Tele2* rejected the idea that Article 15(1) provides a broad exception to the general rule of privacy. It took the position that Directive 2002/58 covered a legislative measure on both the retention of and access to the data [317] because "[t]he protection of the confidentiality of electronic communications and related traffic data, guaranteed in Article 5(1) of Directive 2002/58, applies to the measures taken by *all* persons other than users, whether private persons or bodies or State

---

[314] *See* Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, 28 HARV. HUM. RTS. J. 65 (2015); Orla Lynskey, *The Data Retention Directive is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland*, 51 COMMON MKT. L. REV. 1789 (2014); Arianna Vedaschi & Valerio Lubello, *Data Retention and Its Implications for the Fundamental Right to Privacy*, 20 TILBURG L. REV. 14 (2015); Mark D. Cole & Franziska Boehm, *EU Data Retention—Finally Abolished?: - Eight Years in Light of Article 8*, 97 CRITICAL. Q. FOR LEGIS. & L. 58 (2014); David Eisendle, *Data Retention: Directive Invalid—Limits Imposed by the Principle of Proportionality Exceeded, Constitutional Developments in Austria*, 8 VIENNA J. ON INT'L CONST. L. 458 (2014).

[315] Joined Cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen, ECLI:EU:C:2016:970, ¶¶ 1–134 (Dec. 21, 2016) [hereinafter *Tele2*].

[316] Council Directive 2002/58, art. 15(1), 2002 O.J. (L 201) 37, 46 (EC).

Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in . . . this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e., state security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences . . . To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph[.]

[317] *Tele2, supra* note 315, ¶¶ 75, 76.

bodies."[318] Here the CJEU adopted a bold and innovative broad interpretation of both "measures" and "data" in Directive 2002/58, guided by the principle of confidentiality of electronic communications. While Article 15(1) is an exception,[319] it is an exception that must be interpreted *strictly*.[320] In particular, the CJEU made it explicit that the exception cannot become the rule:

> That provision cannot, therefore, permit the exception to that obligation of principle and, in particular, to the prohibition on storage of data, laid down in Article 5 of Directive 2002/58, to become the rule, if the latter provision is not to be rendered largely meaningless.[321]

In order to make sure Article 15(1) exceptions are not a blank check to the national governments, the CJEU required national measures claimed under Article 15(1) to pass the principle of proportionality test, another key constitutional principle in EU law, which required

> [L]imitations may be imposed on the exercise of those rights and freedoms only if they are necessary and if they genuinely meet objectives of general interest recognized by the European Union or the need to protect the rights and freedoms of others . . .[322]

Therefore, the CJEU in *Tele2* exercised its judicial powers of a constitutional court in recognizing the higher principle of privacy in EU law, and then prescribed procedural safeguards according to the constitutional principle of proportionality.

Similarly, in *La Quadrature*,[323] France was joined by the Czech Republic, Estonia, Ireland, Cyprus, Hungary, Poland, Sweden, and the United Kingdom in claiming that Directive 2002/58 does not cover national legislation on intelligence data gathering.[324] The CJEU disagreed. Based on underlying proprietary rights to data, the CJEU distinguished two kinds of data. One is state-owned data—where the Member States directly engaged in data gathering without imposing processing obligations on providers of electronic communications services. Such data is covered by national law only, not

---

[318] *Id.* ¶ 78 (emphasis added).

[319] *Id.* ¶ 85.

[320] *Id.* ¶ 89 (emphasis added).

[321] *Id.*

[322] *Id.* ¶ 94.

[323] Case C-511/18, C-512/18 and C-520/18, La Quadrature du Net and Others, ECLI:EU:C:2020:791 (Oct. 6, 2020).

[324] *Id.* ¶ 89.

Directive 2002/58.[325] The other is commercial data—where national legislation requires providers of electronic communications services to retain traffic and location data to protect national security and combat crime. Such data fall within the scope of Directive 2002/58.[326]

More recently, in the case of *Commissioner of An Garda Síochána,*,[327] the CJEU shows a consistent position on Article 15. This is a case with a factual pattern similar to that in *Carpenter*. Here, Graham Dwyer was convicted and sentenced to life imprisonment in a murder case.[328] In his appeal, Dwyer alleged that the trial court incorrectly admitted as evidence traffic and location data from his cell phone company—data that were retained in accordance with the Irish Communications (Retention of Data) Act 2011.[329] But the Act, Dwyer alleged, which required general and indiscriminate retention of data, contravened Article 15(1) of Directive 2002/58.[330] The question was ultimately referred to the CJEU. After careful elaboration on the right of privacy and the constitutional principle of proportionality, the CJEU concluded that Article 15(1) does not permit general and indiscriminate retention of traffic and location data;[331] although, *targeted* retention of traffic and location data could be retained when it is limited and strictly necessary.

In sum, through a series of decisions, from *Digital Rights Ireland* (2014), to *Tele2* (2016), and *La Quadrature du Net* (2020), *G.D.* (2022), the CJEU redirected the debates on data retention in the European Union by bringing constitutional norms to the lawmaking process. This was done by a constitutional court exercising judicial review power in *Digital Rights Ireland* (2014), then declaring procedural safeguards derived from the constitutional principle of proportionality. The CJEU provided crucial constitutional constraints on the surveillance states in their access to the data held by private service providers.

IV. OWNERSHIP CONTROL OF DATA IN ILLIBERAL SOCIETIES

The same debate on who owns data is also happening in illiberal societies. This Part surveys three countries: Turkey, Russia, and China. In all the three countries, the internet and social media brought new tools to citizens and civil society in their fight for freedom and democracy. Initially, the internet was

---

[325] *Id.* ¶ 103.

[326] *Id.* ¶ 104.

[327] Case C-140/20, G.D. v. Comm'r of the Garda Síochána, ECLI:EU:C:2022:258 (Apr. 5, 2022).

[328] Some of the factual information is from the Irish Supreme Court decision in *Dwyer*, however the CJEU's ruling hides the full name of the petitioner and used an acronym, unlike how the petitioner's full name was used in Irish courts' rulings. *Id.* ¶¶ 20 (citing Dwyer v. Comm'r of an Garda Síochána [2020] IESC 4 (Ir.)).

[329] *Id.*

[330] *Id.*

[331] *Id.* ¶ 101.

largely private and relatively free in both Turkey and Russia, until the 2012 "Arab Spring," when the ruling elites were alarmed by the power of social media. In China, however, the Party-State tried to take control of the internet earlier, by launching the "Great Firewall of China" shortly after September 11. However, what the three countries have in common is that the surveillance states are more driven by the need for censorship and total control. Thus, the surveillance states are no longer satisfied with access to data collected by private companies. Rather, they want to be the undisputed owners of data. In that sense, illiberal societies are pushing the DCP theory to a new level.

A. Turkey Under Erdogan

Turkey protects privacy as personality rights under Article 25 of the Turkish Civil Code.[332] In this aspect, not only has Turkey transplanted the Continental European notion of personality wholesale in its modern history,[333] but also that it continues to be bound by European Union law as a candidate member, as well as a member of the European Court of Human Rights (ECtHR). The 1982 Turkish Constitution adopted the European Convention of Human Rights, asserting that "everyone has the right to demand respect for his/her private and family life."[334] Turkey also has a Constitutional Court formed under the 1961 Constitution. [335] However, since its founding, the Constitutional Court has never functioned as a guardian of citizens' rights.[336]

---

[332] Tuğrul Ansay, *Law of Persons*, *in* INTRODUCTION TO TURKISH LAW 85, 93 (Don Wallace & Tuğrul Ansay eds., 2005)

> Acts against a person's honor and dignity may also be prevented or stopped under [Article 25] of the Civil Code. Thus, a person may apply to the court when his honor or dignity is damaged by way of accusations, libels, slanders, wrong information or improper criticism." "Disclosing secrets, such as private letters, or listening in on telephone calls of others, or improperly publishing pictures of a person are also considered acts against personality.

[333] Turkey adopted modern civil code in 1926 by transplanting the 1907 Swiss Civil Code into the young RepublicanTurkey. *See* Ruth A. Miller, *The Ottoman and Islamic Substratum of Turkey's Swiss Civil Code*, 11 J. ISLM. STUD. 335 (2000); Umut Ozsu, *Receiving the Swiss Civil Code: Translating Authority in Early Republican Turkey*, 6 INT'L J.L. CONTEXT 63 (2010). The 1926 Civil Code was abolished and replaced by a new one in December 2001. *See* Fethi, Gedikli, *The Voyage of Civil Code of Turkey from Majalla to the Present Day*, 30 ANNALES DE L'UNIVERSITÉ D'ALGER 217, 217–29 (2016).

[334] TURKEY CUMHURIYETI ANAYASASI [CONSTITUTION] July 9, 1961, art. 20 (Turk.).

[335] *Id.* at 145–52.

[336] Ceren Belge, *Friends of the Court: The Republican Alliance and Selective Activism of the Constitutional Court of Turkey*, 40 L. & SOC'Y REV. 653 (2006); Yusuf Şevki Hakyemez, *"Militant Democracy" and the Turkish Constitutional Court*, *in* A ROAD MAP OF A NEW CONSTITUTION FOR TURKEY: ESSAYS IN COMPARATIVE CONSTITUTIONAL LAW 207, 207–37 (Fatih Öztürk et al. eds., 2014) (examining the Constitutional Court's cases on dissolution of political parties and freedom of expression during the 1990s).

In the words of one commentator, it was a "guardian of the regime."[337] In November 2002, Recep Tayyip Erdogan and his pro-Islamist party AKP (Justice and Development Party) won the national election and began to dominate Turkish politics.[338] Initially, Erdogan was moderately conservative on religion;[339] he promised reforms to meet the demands for accession to the European Union.[340] After the European Parliament elections in June 2009, however, accession to the EU became patently hopeless.[341] Erdogan increased his control of the Constitutional Court through amendments to the Constitution in 2010,[342] and the antidemocratic nature of the Court remained unchanged. [343] Before the "Arab Spring," Turkey under Erdogan moved unequivocally towards an autocracy.[344]

In such context, Turkey under Erdogan responded to the rise of the internet and social media by introducing tighter content control. Internet was introduced into Turkey in the early 1990s; citizens began to have access to the

---

[337] Hootan Shambayati, *The Guardian of the Regime: The Turkish Constitutional Court in Comparative Perspective*, *in* CONSTITUTIONAL POLITICS IN THE MIDDLE EAST: WITH SPECIAL REFERENCE TO TURKEY, IRAQ, IRAN AND AFGHANISTAN 99 (Said Amir Arjomand ed., 2008).

[337] *Id.*

[338] *Id.*

[339] CARTER VAUGHN FINDLEY, TURKEY, ISLAM, NATIONALISM, AND MODERNITY: A HISTORY (2010).

[340] Fernanda G. Nicola, *Promises of Accession: Reassessing the Trade Relationship Between Turkey and the European Union*, 24 AM. U. INT'L L. REV. 739 (2009); Patrick R. Hugg, *The Republic of Turkey in Europe: Reconsidering the Luxembourg Exclusion*, 23 FORDHAM INT'L L.J. 606 (2000); YONAH ALEXANDER ET AL., TURKEY: TERRORISM, CIVIL RIGHTS, AND THE EUROPEAN UNION (2008) (Negotiation documents have been collected in this book).

[341] Patrick R. Hugg, *Accession Aspirations Degenerate: A New Chapter for Turkey and the E.U.*, 9 WASH. U. GLOBAL STUD. L. REV. 225 (2010).

[342] This was achieved through a constitutional referendum in September 2010, which substantially weakened the Kemalist control of the judiciary. *See* Asli Ü. Bâli, *The Perils of Judicial Independence: Constitutional Transition and the Turkish Example*, 52 VA. J. INT'L L. 235 (2012); A. Serra Cremer, Comment, *Turkey Between the Ottoman Empire and the European Union: Shifting Political Authority Through Constitutional Reform*, 35 FORDHAM INT'L L.J. 279 (2011); Ergun Özbudun, *Turkey's Search for a New Constitution*, 14 INSIGHT TURK. 39, 39–50 (2012).

[343] Ozan O. Varol et al., *An Empirical Analysis of Judicial Transformation in Turkey*, 65 AM. J. COMP. L. 187 (2017) (noting a conservative ideological shift between 2007 and 2014, based on survey of 200 cases ruled by the Constitutional Court); Omar El Manfalouty, *Authoritarian Constitutionalism in the Islamic World: Theoretical Considerations and Comparative Observations on Syria and Turkey*, *in* AUTHORITARIAN CONSTITUTIONALISM: COMPARATIVE ANALYSIS AND CRITIQUE (Helena Alviar et al. eds., 2019).

[344] Merve Tahiroglu, *How Turkey's Leaders Dismantled the Rule of Law*, 44 FLETCHER F. WORLD AFF. 67 (2020); Felix Petersen & Zeynep Yanaşmayan, *Explaining the Failure of Popular Constitution Making in Turkey (2011-2013)*, *in* THE FAILURE OF POPULAR CONSTITUTION MAKING IN TURKEY: REGRESSING TOWARDS CONSTITUTIONAL AUTOCRACY 21–56 (2019); Halil Karaveli, *Erdogan's Journey: Conservatism and Authoritarianism in Turkey*, 95 FOREIGN AFF. 121 (2016).

internet in 1996.[345] This coincided with media privatization in Turkey.[346] Türk Telekom (TT), which had a monopoly over internet access, was privatized in 2006.[347] In March 2007, YouTube was temporarily blocked after an Istanbul court found videos on YouTube insulting Atatürk.[348] Soon after the incident, the Parliament, controlled by the AKP, passed Law No. 5651, known as the Internet Law in Turkey,[349] giving courts the power to issue orders to block any website where there was "sufficient suspicion" a crime had occurred. Blocking became powerful leverage that Erdogan used to control social media.[350] On May 15, 2011, during the Taksim Square march, social media proved essential, not only for the mobilization of protestors, but also for reporting and discursive construction of the protests.[351] After the Arab Spring, control of cyberspace only intensified. For its role during the Gezi Park protests in May 2013, Twitter was banned in 2014.[352]

During this period, Erdogan drastically transformed the domestic media. By 2020, "[m]ore than 90 percent of [Turkey's] conventional media is now

---

[345] ERKAN SAKA, SOCIAL MEDIA AND POLITICS IN TURKEY: A JOURNEY THROUGH CITIZEN JOURNALISM, POLITICAL TROLLING, AND FAKE NEWS 3 (2019).

[346] Ayşe Öncü, *Rapid Commercialization and Continued Control: The Turkish Media in the 1990s*, *in* TURKEY'S ENGAGEMENT WITH MODERNITY: CONFLICT AND CHANGE IN THE TWENTIETH CENTURY 388–402 (C. Kerslake et al. eds., 2010).

[347] SAKA, *supra* note 345, at 4.

[348] Tom Zeller, Jr., "YouTube Banned in Turkey After Insults to Ataturk," Mar. 7, 2007, available at: https://archive.nytimes.com/thelede.blogs.nytimes.com/2007/03/07/youtube-banned-in-turkey-after-insults-to-ataturk/. Nicole Wong, Deputy General Counsel of Google, Inc., testified at a United States Senate hearing that "YouTube has been blocked in Turkey repeatedly over the past year [2007] because of videos deemed insulting to Mustafa Kemal Ataturk, the founding father of modern Turkey, and other videos deemed by the Turkish government to be threatening to the state, such as videos promoting an independent Kurdistan." *Testimony of Nicole Wong, Deputy General Counsel, Google Inc*., in GLOBAL INTERNET FREEDOM: CORPORATE RESPONSIBILITY AND THE RULE OF LAW: HEARING BEFORE THE SUBCOMMITTEE ON HUMAN RIGHTS AND THE LAW OF THE COMMITTEE ON THE JUDICIARY UNITED STATES SENATE 144 (2nd Sess., Ser. No. J-110-93) (May 20, 2008).

[349] Law on Regulation of Broadcasts via Internet and Combatting Crimes Committed by Means of Such Publications, Law No.: 5651, 25 Mar. 2007 No. 26530, enacted 04 May 2007 (Turk.).

[350] The best-known case was Ahmet Yildirim, an academic living in Istanbul who owned and ran a website. In June 2009, he was accused of insulting the memory of Atatürk, and a local criminal court issued an order blocking Yildirim's website based on Law No. 5651. The ECtHR clashed with the efforts to block access to the internet. Yildirim v. Turkey, App. No. 3111/10 (Dec. 18, 2012), https://hudoc.echr.coe.int/fre?i=002-7328; *see also* Cengiz v. Turkey, App. Nos. 48226/10 & 14027/11 (Dec. 1, 2015), https://hudoc.echr.coe.int/eng?i=001-159188.

[351] SAKA, *supra* note 345, at 13.

[352] Prasant Naidu, *The Twitter War in Turkey*, SOC. MEDIA TODAY (Apr. 24, 2014), https://www.socialmediatoday.com/content/twitter-war-turkey; *see also,* Jeffery Wilson & Ashley Hahn, *Twitter and Turkey: Social Media Surveillance at the Intersection of Corporate Ethics and International Policy*, 11 J. INFO. POL'Y 444 (2021).

controlled by conglomerates" loyal to the AKP.[353] He also deployed surveillance, including interception of communications,[354] and criminal penalties for online postings,[355] to control protestors, journalists, and other activists in Turkey. However, the most popular social media sites in Turkey were created by foreign companies like Twitter, which have no physical presence in Turkey.[356] On July 29, 2020, Turkish Parliament amended Law No. 5651, requiring social media platforms with over one million daily users to open an office in Turkey, and to store user data inside Turkey.[357] In March 2021, Twitter agreed to comply with the requirements.[358] The decision indicates Twitter's shift of identity, from a public platform serving citizens' freedom to that of a business enterprise whose primary purpose is profits.[359]

B. Russia under Putin

Like Turkey, the internet in Russia started as a private industry. In December 1991, Boris Yeltsin opened the door for privatization in the mass media sector.[360] The Runet startups took advantage of this more open environment. Yandex, Russia's most popular search engine, was founded in 1997. VKontakte, one of the most popular social network apps, was founded in 2006.[361] Similarly, LiveJournal was acquired by a private Russian company in

---

[353] Marc Santora, *Turkey Passes Law Extending Sweeping Powers Over Social Media*, N.Y. TIMES (July 29, 2020), https://www.nytimes.com/2020/07/29/world/europe/turkey-social-media-control.html.

[354] Tanrikulu v. Turkey, App. No. 27473/06, ¶ 37 (July 18, 2017), https://hudoc.echr.coe.int/eng?i=001-175464.

[355] Şorli v. Turkey, App. No. 42048/19, Eur. Ct. H.R. (2021). ECtHR rulings have limited de facto impact in Türkey. *See* Ergun Özbudun & Füsun Türkmen, *Impact of the ECtHR Rulings on Turkey's Democratization: An Evaluation*, 35 HUM. RTS. Q. 985 (2013).

[356] Wilson & Hahn, *supra* note 352, at 459–61.

[357] Kayahan Cantekin, *Turkey: Parliament Passes Law Imposing New Obligations on Social Media Companies*, LIBR. OF CONG. (Aug. 6, 2020), https://www.loc.gov/item/global-legal-monitor/2020-08-06/turkey-parliament-passes-law-imposing-new-obligations-on-social-media-companies/.

Kim Lyons, *Twitter Will Set up a Legal Entity in Turkey to Comply with Controversial Social Media Law*, THE VERGE (Mar. 20, 2021, 11:24 AM), https://www.theverge.com/2021/3/20/22341798/twitter-legal-entity-turkey-comply-social-media-law-privacy.

[359] *See* Wilson & Hahn, *supra* note 352, at 459–61.

[360] Law of the Russian Federation on Mass Media (No.2124-1 /1991), ART. 1 (Russ.). For the early stage of the privatization of the television and radio sectors, see Michael J. Bazyler & Eugene Sadovoy, *Government Regulation and Privatization of Electronic Mass Media in Russia and the Other Former Soviet Republics*, 14 WHITTIER L. REV. 427 (1993). *But see* OLESSIA KOLTSOVA, NEWS MEDIA AND POWER IN RUSSIA 77 (2006) (noting, "[t]he early 1990s was a brief period of conversion of media into what was planned to be a classical internal private ownership. The late 1990s, on the contrary, were dominated by nationalization of media.").

[361] Natalia Konradova, *The Rise of Runet and the Main Stages of Its History*, *in* INTERNET IN RUSSIA: A STUDY OF THE RUNET AND ITS IMPACT ON SOCIAL LIFE 39–63 (Sergey Davydov ed., 2020).

2006.[362] Even politically, this was a relatively liberal period. The 1993 Constitution recognizes privacy rights, following the wording of the European Human Rights Convention.[363] Russia joined the Council of Europe on February 28, 1996.[364] Vladimir Putin was appointed prime minister in August 1999 and became President of the Russian Federation in May 2000. Until 2012, Putin's Russia sought cooperative relations with the European Union and even to join NATO (the North Atlantic Treaty Organization).[365]

Domestic protests during the December 2011 parliamentary election,[366] the March 2012 presidential election in Russia,[367] and the "Twitter Revolution" during the "Arab Spring" changed the perception of the ruling elites in Russia. Now the internet was considered a tool of United States expansionism, "content as threat,". Thus in 2012 Putin started talking about "digital sovereignty."[368] An immediate shift in internet policy was content control. In November 2012, a blacklist system called "Single Register" was introduced, which required internet service providers to block access to the websites on the blacklist.[369] In December 2013, the same power was extended to websites that

---

[362] *Id.*

[363] KONSTITUTSIIA ROSSIĬSKOĬ FEDERATSII [KONST. RF] [CONSTITUTION] art. 23(1), 24(1) (Russ.). Article 23(1) provides, "[e]veryone shall have the right to the inviolability of private life, personal and family privacy, and protection of honor and good name." *Id.* art. 23(1). Article 24(1) provides: "[t]he collection, keeping, use and dissemination of information about the private life of a person shall not be allowed without his or her consent." *Id.* art. 24(1).

[364] Bill Bowring, *Russia's Accession to the Council of Europe and Human Rights: Four Years On*, 11 HELSINKI MONITOR 53 (2000).

[365] TIMOTHY SNYDER, THE ROAD TO UNFREEDOM: RUSSIA, EUROPE, AMERICA 79 (2018).

[366] For example, Mr. Aleksey Navalnyy, the anti-corruption campaigner and popular blogger, was arrested in the December 2011 protest after taking part in a public demonstration in Moscow. Eventually, the European Court of Human Rights found multiple violations of the European Convention of Human Rights. *See* Navalnyy and Yashin v. Russia, App. No. 76204/11, Eur. Ct. H.R. (Dec. 4, 2014).

[367] Mr. Aleksey Navalnyy was arrested again in March 2012 after taking part in a public meeting at Pushkinskaya Square in Moscow. The Grand Chamber of the European Court of Human Rights found multiple violations of the European Convention of Human Rights. Navalnyy v. Russia, App. No. 29580/12, ¶ 1 (Nov. 15, 2018), https://hudoc.echr.coe.int/eng?i=001-187605 (endorsing the findings of the Third Section of ECtHR in its earlier ruling in Navalnyy v. Russia, App. No. 29580/12, ¶ 6 (Feb. 2, 2017), https://hudoc.echr.coe.int/eng?i=001-170655).

[368] Alexandra V. Orlova, *"Digital Sovereignty," Anonymity and Freedom of Expression: Russia's Fight to Re-Shape Internet Governance*, 26 U.C. DAVIS J. INT'L L. & POL'Y 225, 230-31 (2020).

[369] Federal'nyĭ Zakon RF o Grazhdanstve Rossiĭskoĭ Federatsii [Federal Law of the Russian Federation on Citizenship of the Russian Federa- tion], Sobranie Zakonodatel'stva Rossiĭskoĭ Federatsii [SZ RF] [Russian Federation Collection of Legislation] 2012, No. 139, Item FZ (granting government agencies the power to blacklist websites containing child pornography, advocacy of drug abuse and suicide). *See also* Tatiana Brazhnik, *Russia: Evolution and Main Trends in Informational Law* (Feb. 27, 2013), https://ssrn.com/abstract=2359152; Andrei Soldatov & Irina Borogan, *Russia's Surveillance State*, 30 WORLD POL'Y J. 23, 28 (2013).

contained "harmful" information.[370] In May 2014, all bloggers with posts that exceeded 3,000 visits were required to register with the government.[371] In September 2014, all internet service providers were required to store the personal data of Russian citizens in Russia.[372]

However, blocking websites can be costly. First, it is legally and politically costly when a blocking order is declared a breach of Article 11 of the European Convention on Human Rights,.[373] Second, the Russian government soon encountered resistance from privately-owned internet service providers.[374] Western social media companies such as Facebook, Google, Twitter, and Telegram Messenger, a British firm, occasionally resisted censorship orders.[375] Similarly, Russia has made similar demands of privately-owned Russian companies, but these companies have also resisted. In 2014, the newspaper Novaya Gazeta, one of the leading mass media companies operating the website novayagazeta.ru, refused to remove an article that had been considered "extremist speech" and even challenged the government warning

---

[370] Federal'nyĭ Zakon RF o Grazhdanstve Rossiĭskoĭ Federatsii [Federal Law of the Russian Federation on Citizenship of the Russian Federa- tion], Sobranie Zakonodatel'stva Rossiĭskoĭ Federatsii [SZ RF] [Russian Federation Collection of Legislation] 2013, No. 398, Item FZ (granting Roskomnadzor (the Russian Federal Service for Supervision of Communications, Information Technology, and Mass Media) power to blacklist websites publishing "extremist" speeches).

[371] Federal Law No. 97-FZ (Bloggers Law), May 5, 2014, an English summary is available at: https://wilmap.stanford.edu/entries/federal-law-no-97-fz-bloggers-law. For commentaries, Neil MacFarquhar, *Russia Quietly Tightens Reins on Web With "Bloggers Law*," N.Y. TIMES, May 6, 2014, https://www.nytimes.com/2014/05/07/world/europe/russia-quietly-tightens-reins-on-web-with-bloggers-law.html; Oleg Soldatov, *Half-Hearted Inception, Miserable Existence, and the Untimely Death of the Bloggers' Register in Russia*, 52 ISR. L. REV. 61 (2019).

[372] Federal Law No. 242-FZ (Data Localization Law), Jul. 21, 2014, took effect on Sept. 1, 2015. English translation is available at https://ccsp.alukos.com/laws/federal-law-no-242-fz/.

[373] OOO Flavus v. Russia, App. No. 12468/15, ¶ 1 (Jun. 23, 2020), https://hudoc.echr.coe.int/fre?i=002-12858 (Prosecutor General identified websites owned and operated by Flavus, Kasparov, and Mediafokus for mass disorder, extremist activities or participation in unauthorized mass gatherings, and sent a blocking request directly to Roskomnadzor, the telecommunication agency. Roskomnadzor subsequently blocked the websites. In November 2020, the European Court of Human Rights found the blocking of websites in violation of the European Convention. *See also* Kablis v. Russia, App. No. 48310/16, (Sept. 09, 2019), https://hudoc.echr.coe.int/eng?i=001-192769.

[374] Markku Lonkila noted that during the winter of 2011-2012 demonstrations, VKontakte founder Pavel Durov was approached by the Federal Security Service, asking him to shut down some opposition groups. Durov refused but was forced to sell his shares and emigrate in 2014. Markku Lonkila, *Social Network Sites and Political Governance in Russia*, *in* AUTHORITARIAN MODERNIZATION IN RUSSIA: IDEAS, INSTITUTIONS AND POLICIES 113, 118 (Vladimir Gel'man ed., 2017).

[375] *See* Andrei Zakharov & Ksenia Churmanova, *How Russia Tries to Censor Western Social Media*, BBC (Dec. 17, 2021), https://www.bbc.com/news/blogs-trending-59687496. *See also* Telegram Messenger LLP v. Russia, App. No. 13232/18, ¶¶ 9–12 (Oct. 29, 2020), https://hudoc.echr.coe.int/eng?i=001-206288 (Telegram Messenger, a British firm having operation in Russia through its messaging application, resisted a disclosure order from the Federal Security Service ("FSB"), and lodged a complaint to the ECtHR).

notice in court.[376] Similarly, in March 2014, Grani.Ru, an oppositional online media, was blocked for publishing articles calling for taking part in a public meeting that the government considered problematic. Grani.Ru filed a lawsuit in court challenging the government.[377] Grani.Ru did not win the case in the Moscow court, but prevailed in the European Court of Human Rights against the Russian government.[378]

Therefore, the Russian government adopted a different strategy—control through ownership. According to Professor Carolina Pallin, a Swedish scholar based in Stockholm, Russia brought internet infrastructure either by direct state-owned companies or indirect control through companies owned by people with close connections and loyalties to the political leadership.[379] This is in the area of broadband cable services and domain name registration; for example, some of the most popular social network sites like VKontakte, or the search engine Yandex, have mixed ownership.[380] Pallin observed that "[o]verall, the business empires that owned the most important Internet websites by 2015 in Russia are part of the *sistema*."[381] In 2016, Roskomnadzor—the Russian government agency—joined Netoscope and other private tech firms to form a "public-private partnership."[382]

Shortly before the invasion of Ukraine in February 2022, efforts to control the internet in Russia intensified. In December 2021, VKontakte was taken over by two subsidiaries of Gazprom, the state-owned gas giant.[383] After the invasion, Russia intensified its control of the internet and social media. It blocked Instagram, calling it an "extremist organization" for allowing statements critical of the invading Russian troops.[384] While the autocratic regime continues using regulatory control, direct control by ownership seems

---

[376] Liudmila Sivetc, *State Regulation of Online Speech in Russia: The Role of Internet Infrastructure Owners*, 27 INT'L J.L. & INFO. TECH. 28, 37–38 (2018).

[377] *Id.* at 41-42.

[378] OOO Flavus v. Russia, App. No. 12468/15, *supra* note 373 (Applicant OOO Flavus was the owner of Grani.Ru).

[379] Carolina Vendil Pallin, *Internet Control Through Ownership: The Case of Russia*, 33:1 POST-SOVIET AFF. 16, 21 (2017).

[380] *Id.* at 23.

[381] *Id.* at 24. "Sistema" means informal power networks, *see*, ALENA V. LEDENEVA, CAN RUSSIA MODERNISE? SISTEMA, POWER NETWORKS AND INFORMAL GOVERNANCE (Cambridge 2013).

[382] Sivetc, *supra* note 376, at 45.

[383] Sarah E. Needleman & Evan Gershkovich, *Kremlin Promotes Domestic Social-media Platforms*, WALL ST. J., April 21, 2022, at A5; *The Russian Stack*, ECONOMIST, Feb. 19, 2022, at 58.

[384] Sam Schechner & Keach Hagey, *Russia Expands Social Media Bans*, WALL ST. J., Mar. 14, 2022, at A7; *see also* Sam Schechner, *Google News Is Restricted in Russia*, WALL ST. J., Mar. 25, 2022, at A10.

to be an indispensable approach.[385] In its efforts to tame the internet, Russia has much in common with other illiberal societies like Turkey and China.[386]

C. China under Xi Jinping

For most observers in the West, China represents the prototype of the modern surveillance state in cyberspace.[387] China's "Great Firewall," a censorship and surveillance system developed in the early 2000s, has become a sophisticated censorship machine.[388] Today, China exports its surveillance technology to other authoritarian regimes across the globe.[389] Like other surveillance states, the Party-State in China also wants data from tech companies. Under President Xi Jinping, the Party-State's thirst for data and distrust of private property drove the push for more direct control.

1. The Great Firewall of China

The internet was introduced in China in 1987, and internet service became open to the general public in 1995.[390] The Chinese government has taken an active and influential role in promoting the internet since the 1990s.[391] The telecommunication sector was reformed in this period. China Unicom (中国联

---

[385] The government began requiring internet service providers (ISPs) to install hardware that blocks Tor, a tool widely used in Russia to mask online activity, *ibid*. Soon after the invasion was launched, Russia started restricting access to Twitter, Instagram, and passed new "fake news" laws, punishing dissemination of information considered "unreliable." Ugolovnyĭ Kodeks Rossiĭskoĭ Federatsii [UK RF] [Criminal Code] Nos. 31–FZ and 32-FZ (Russ.).

[386] In fact, Putin's Russia and Xi Jinping's China often acted in concert on "digital sovereignty," see, Stanislav Budnitsky & Lianrui Jia, *Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance*, 21 EUR. J. CULTURAL STUD. 594 (2018).

[387] *See* JOSH CHIN & LIZA LIN, SURVEILLANCE STATE: INSIDE CHINA'S QUEST TO LAUNCH A NEW ERA OF SOCIAL CONTROL (2022); Paul Mozur & Aaron Krolik, *China's Blueprint for a Digital Totalitarian State*, N.Y. TIMES, Dec. 18, 2019, at A1; Kenneth Roth & Maya Wang, *Data Leviathan: China's Burgeoning Surveillance State*, N.Y. REV. (Aug. 16, 2019), https://www.nybooks.com/daily/2019/08/16/data-leviathan-chinas-burgeoning-surveillance-state/.

[388] ELIZABETH C. ECONOMY, THE THIRD REVOLUTION: XI JINPING AND THE NEW CHINESE STATE (2018) [hereinafter, ECONOMY, THE THIRD REVOLUTION]. One recent incident is just another reminder of how this censorship machinery is deeply embedded in people's daily life, see Coco Feng, *Software Firm Faces "Crisis of Trust" Over Alleged Censorship*, S. CHINA MORNING POST, Jul. 15, 2022, at A8 (describing how a novelist in China found her written work on her computer locked by the word processing software WPS).

[389] Samuel Woodhams, *China, Africa, and the Private Surveillance Industry,* 21 GEO. J. INT'L AFF. 158, 159 (2020); Paul Mozur et al., *A Chinese Export Creeps In. And It's Watching*, N.Y. TIMES, Apr. 25, 2019, at A1 (describing the exportation of Chinese surveillance technology and equipment to Ecuador).

[390] The first commercial internet service was launched in May 1995 in Beijing when Beijing Telecom introduced the ChinaNet-branded service. Similar services became available in June 1995 in Shanghai, and then in Guangdong, Liaoning and Zhejiang in the second half of 1995. *See*, Eric Harwit & Duncan Clark, *Shaping the Internet in China: Evolution of Political Control over Network Infrastructure and Content*, 41 ASIAN SURV. 377, 382, 388 (2001); ERIC HARWIT, CHINA'S TELECOMMUNICATIONS REVOLUTION (2008) (hereinafter, CHINA'S TELECOM).

[391] HARWIT, CHINA'S TELECOM, *id*., Chapter 4 (China's Internet and Government Policy).

通) was formed in July 1994.[392] In May 2000, though still state-owned, China Mobile (中国移动) gained more independence in its operations by a separation from its parent company, China Telecom.[393] Alibaba was founded in 1999 in Hangzhou,[394] Tencent in 1998 in Shenzhen,[395] Sina in 1998 in Beijing,[396] and Baidu in 2000 in Beijing—all are private companies.[397]

According to Elizabeth Economy, a China specialist based in the U.S., "[i]nternet activism in China exploded during the final years of Hu Jintao's tenure. The Chinese people logged on to engage in lively political social discourse, to gain access to the world outside China, and to organize themselves to protest against perceived injustices."[398] Before September 11, China was already facing issues: the religious sect *Falungong* (April 1999), the China Democracy Party (June 1998), Tibetan protests,[399] social protests on environmental pollution, land-takings, and consumer movements.[400] In response, the "Golden Shield" project was started in 1996 and completed around 1999.[401] This later became known as the "Great Firewall of China." In building the system, China received capable assistance from Western tech companies. Cisco Systems, Inc., the American maker of routers, switches that were essential for internet filtering, became a close partner to China.[402] Cisco started selling firewall boxes to China in 1997, and won contracts to deploy

---

[392] Eric Harwit, *China's Telecommunications Industry: Development Patterns and Policies*, 71 PAC. AFFS. 175, 189 (1998); HARWIT, CHINA'S TELECOM, *id*. at 48.

[393] Eric Harwit, *China's Telecommunications Industry: Development Patterns and Policies*, 71 PAC. AFFS. 175 (1998); HARWIT, CHINA'S TELECOM, *supra* note 391, at 68.

[394] DUNCAN CLARK, ALIBABA: THE HOUSE THAT JACK MA BUILT 93 (2016) [hereinafter, CLARK, ALIBABA].

[395] MIN TANG, TENCENT: THE POLITICAL ECONOMY OF CHINA'S SURGING INTERNET GIANT 23 (2020).

[396] *Id.* at 21.

[397] *Id.* at 23.

[398] ECONOMY, THE THIRD REVOLUTION, *supra* note 388, at 77.

[399] MICHAEL CHASE & JAMES MULVENON, YOU'VE GOT DISSENT! CHINESE DISSIDENT USE OF THE INTERNET AND BEIJING'S COUNTER-STRATEGIES 1–44 (2002).

[400] THE INTERNET, SOCIAL MEDIA, AND A CHANGING CHINA (Jacques de Lisle et al. eds., 2016); Eric Harwit, *The Rise and Influence of Weibo (Microblogs) in China*, 54 ASIAN SURV. 1059 (2014); Rebecca MacKinnon, *Flatter World and Thicker Walls? Blogs, Censorship and Civic Discourse in China*, 134 PUB. CHOICE 31 (2008).

[401] SONALI CHANDEL, ET. AL., THE GOLDEN SHIELD PROJECT OF CHINA: A DECADE LATER—AN IN-DEPTH STUDY OF THE GREAT FIREWALL 111–19 (2019); ECONOMY, THE THIRD REVOLUTION, *supra* note 388, at 71.

[402] The OpenNet Initiative, a civic internet NGO, concluded in April 2005 that the core of China's Internet relies on Cisco technology. OpenNet Initiative, *Internet Filtering in China in 2004-2005: A Country Study,* in CHINA'S STATE CONTROL MECHANISMS AND METHODS 171; *Hearing before the U.S.-China Econ. and Sec. Rev. Comm'n*, 109th Cong. (2005).

PoliceNet, the Chinese State security system by 2003.[403] Another partner was Nortel Networks Corporation, the Canadian network company, which formed a joint venture in Guangdong province in 1995, and was actively involved in the Great Firewall project in the early 2000s.[404]

The first legal framework for data retention in China was developed in this context. In September 2000, the Chinese government issued two related administrative laws which constituted the legal framework for the internet: Telecommunications Regulations,[405] and the Administrative Measures on Internet Information Services.[406] Both required data retention.[407] In February 2006, the Ministry of Information Industry publicized its rule for internet email services.[408] Article 10 provided similar duties for Internet email service providers to retain data on the times of transmission or reception, email addresses, IP addresses of the senders, and recipients of the emails.[409]

American tech companies such as Google, Microsoft, and Yahoo came to China to explore its market. Yahoo launched its operation in China in 1999

---

[403] *Hearing before the Subcomm. on Afr., Global Hum. Rts. and Int'l Operation of the H. Comm. on Int'l Rels.* 109th Cong. (2006). (Statement of Ethan Gutmann); *see also* GLOBAL INTERNET FREEDOM: CORPORATE RESPONSIBILITY AND THE RULE OF LAW (Hearing before the Subcommittee on Human Rights and the Law of the Committee on the Judiciary, U.S. Senate) (May 20, 2008). Cisco's involvements in China's internet filtering were also revealed in legal briefs in subsequent legal actions against Cisco. *See* Doe v. Cisco Sys., 66 F.Supp.3d 1239 (N.D. Cal. 2014); Du Daobin v. Cisco Sys., 2 F.Supp.3d 717 (D. Md. 2014).

[404] GREG WALTON, CHINA'S GOLDEN SHIELD: CORPORATIONS AND THE DEVELOPMENT OF SURVEILLANCE TECHNOLOGY IN THE PEOPLE'S REPUBLIC OF CHINA 18 (International Center for Human Rights and Democratic Development 2001); Didi Kirsten Tatlow, et al., *The Impact of China's Policies*, *in* CHINA'S QUEST FOR FOREIGN TECHNOLOGY: BEYOND ESPIONAGE 205–22 (William C. Hannas & Didi Kirsten Tatlow eds., 2020).

[405] Zhonghua Renmin Gongheguo Dianxin Tiaoli (中华人民共和国电信条例) [Regulation of the People's Republic of China on Telecommunications], (promulgated by Order No. 291 of the State Council of the People's Republic of China, Sep. 25, 2000), http://www.gov.cn/zhengce/2020-12/26/content_5574368.htm, *translated in Telecommunications Regulations*, 48 CHINESE L. & GOV'T 15 (2016) [hereinafter, 2000 Telecom Regulations].

[406] Hulianwang Xinxi Fuwu Guanli Banfa (互联网信息服务管理办法) [Measures for the Administration of Internet Information Services], (promulgated by Order No. 292 of the State Council of the People's Republic of China, Sep. 25, 2000, rev'd by the State Council on Abolishing and Amending Some Administrative Regulations, Jan. 8, 2011), http://www.gov.cn/zhengce/2020-12/26/content_5574367.htm.

[407] Article 62 of the 2000 Telecom Regulations, *supra* note 405; Article 16 of the 2000 Internet Measures, *id.*

[408] Hulianwang Dianzi Youjian Fuwu Guanli Banfa (互联网电子邮件服务管理办法) [Measures for the Administration of Internet E-mail Services], (promulgated by Order No.38 of Ministry of Indus. and Info. Tech. of China, Feb. 20, 2006, effective Mar. 30, 2006), http://www.gov.cn/ziliao/flfg/2006-03/06/content_219353.htm, Mar. 06, 2006, *translated in Measures for the Administration of Internet E-mail Services*, 48 CHINESE L. & GOV'T 173 (2016).

[409] *Id.* art. 10.

and became a major shareholder of Alibaba in May 2005.[410] A series of high-profile cases, including that of journalist Shi Tao (师涛), revealed the operational principles of these tech companies. Shi Tao was a political dissident in China who was arrested by police in November 2004 after being tipped by Yahoo with the subscriber information, private email records, copies of email messages, and other information.[411] In a similar case of Li Zhi (李智), the ruling by the Sichuan Provincial High Court on February 26, 2004,[412] sheds some light on this. Li Zhi was charged with the same crime—subversion against the State, based on his statements and essays published online. Prosecutors presented evidence from three internet service providers: the Beijing Sina.com, Yahoo Hong Kong, and Sichuan Telecom, the local company. They all provided subscriber information, including username, email address, and Internet Protocol (IP) address, which helped identify Li Zhi.[413] Yahoo's cases showed how the Chinese government successfully used its market as leverage to co-opt American tech companies to serve the interests of the surveillance state.[414]

2. From Regulatory to Ownership Control

When he came to power in 2012, Xi Jinping was apt at using law as a tool for controlling the internet.[415] Four major national statutes have been enacted for these purposes. The first was the Anti-Terrorism Act (2015) ("ATA").[416] Article 19 followed the approach of the 2000s in requiring the telecommunication and internet service providers to keep a record of extremist

---

[410] Sue Decker, *An Insider's Account of the Yahoo-Alibaba Deal*, HARV. BUS. REV. (Aug. 6, 2014), https://hbr.org/2014/08/an-insiders-account-of-the-yahoo-alibaba-deal; CLARK, *supra* note 394, at 181–206. 394.

[411] The court ruling of Shi Tao's case has been, most likely, deleted by the Chinese government. However, the case was widely discussed. *See* William Thatcher Dowell, *The Internet, Censorship, and China*, 7 GEO. J. INT'L AFF. 111 (2006). Some of the details in Shi Tao's case were recorded in legal briefs in subsequent litigation in the United States. *See* Wang Xiaoning v. Yahoo!, Inc., No. C 07–2151 CW, 2007 WL 9812491 (N.D. Cal. Oct. 31, 2007); Knopf v. Semel, No. C 08–3658 JF, 2010 WL 965308 (N.D. Cal. Mar. 17, 2010).

[412] Sichuan Sheng Gaoji Renmin Fayuan Xingshi Panjueshu (四川省高级人民法院刑事判决书 [Criminal Judgement of Sichuan Provincial Higher People's Court], Chuan Xing Zhong No. 43, 川刑终字第43号 (2004) (Feb. 26, 2004) (China).

[413] *Id.*

[414] THE INTERNET IN CHINA: A TOOL FOR FREEDOM OR SUPPRESSION (*Hearing before the Subcomm. on Afr., Global Hum. Rights and International Operations and the Subcomm. on Asia and the Pacific of the Comm. on Int'l Relations*, 1?? Cong.) (Feb. 15, 2006); HUMAN RIGHTS WATCH, "RACE TO THE BOTTOM": CORPORATE COMPLICITY IN CHINESE INTERNET CENSORSHIP (2006); G. Elijah Dann & Neil Haddow, *Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! and the Business of Censoring China's Internet*, 79 J. BUS. ETHICS 219 (2008).

[415] Taisu Zhang & Tom Ginsburg, *China's Turn toward Law*, 59 VA. J. INT'L L. 306 (2019).

[416] Zhonghua Renmin Gongheguo Fan Kongbuzhuyi Fa (中华人民共和国反恐怖主义法) [Counterterrorism Law of the People's Republic of China], (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 27, 2015, effective Jan. 1, 2016), 2016 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ.

content once discovered.[417] Article 18 directs service providers to "provide technical interfaces, decryption, and other technical support" to the police and intelligence agency.[418] Under Article 51, the police have the authority to request (*diaoqu*, 调取) relevant information from entities and individuals.[419] The second national statute is the Cybersecurity Act (2016) ("CSA").[420] Article 47 of the Act expands the data retention in Article 19 of ATA to any content violating laws or administrative regulations.[421] Article 28 of the Act, similar to ATA Article 18, requires service providers to provide technical support to the police and intelligence agency.[422] CSA also created China's first data localization rule. Article 37 requires "critical (关键) information infrastructure operators" to store personal data collected and generated in China within the borders of China.[423] Western companies operating in China have no other choice but to comply; in May 2021, both Apple and Tesla opened data centers in China due to the CSA.[424]

The third national statute is the Data Security Law (2021) ("DSL").[425] Article 35 of the Act repeated the general responsibility of Article 51 of ATA, but expanded it to include the authority to request data for the purpose of national security or criminal investigation.[426] To further strengthen the duty under Article 35, Article 48 grants the competent authorities the power to impose the penalty of a warning, and a fine.[427]

---

[417] *Id*. art. 19.

[418] *Id*. art. 18.

[419] *Id*. art. 51.

[420] Zhonghua Renmin Gongheguo Wangluo Anquan Fa (中华人民共和国网络安全法) [The Cybersecurity Law of the People's Republic of China], (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective Jun. 1, 2017), 2016 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 899, *translated in 2016 Cybersecurity Law*, CHINA L. TRANSLATE (NOV. 7, 2016), https://www.chinalawtranslate.com/en/2016-cybersecurity-law/.

[421] *Id*. art. 47.

[422] *Id*. art. 28.

[423] *Id*. art. 37. This was repeated in Article 40 of the more recently enacted PDPA.

[424] Jack Nicas et al., *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, N.Y. TIMES (May 17, 2021), https://www.nytimes.com/2021/05/17/technology/apple-china-censorship-data.html (reporting on Apple); Trefor Moss, *Tesla to Store Data in China Locally*, WALL ST. J., May 27, 2021, at B3 (reporting on Telsa).

[425] Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [People's Republic of China Data Security Law], (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021) 2021 STANDING COMM. NAT'L PEOPLE'S CONG. GAZ. 951. *translated in Data Security Law of the PRC*, CHINA L. TRANSLATE (June 10, 2021), https://www.chinalawtranslate.com/en/datasecuritylaw/.

[426] *Id*. art. 35.

[427] *Id*. art. 48.

The fourth national statute, the Personal Data Protection Act ("PDPA"),[428] was enacted two months after the DSA. PDPA provides more detailed rules on cross-border data transfer through a security review process.[429] It tries to limit and regulate tech companies' collection of data by requiring them to obtain users' consent[430] and give notice to users about their rights.[431] PDPA also explicitly requires that government agencies to follow the same rules when they are engaged in data collection.[432]

However, the Chinese government does not appear to be satisfied with exercising its *regulatory* powers. In 2017, it had discussions with Tencent, Weibo, and a subsidiary of Alibaba about "special management shares."[433] This scheme would have let the government purchase one percent of the companies' shares; in exchange, the investors could appoint a government official to each company's board have a say in its operations. Similarly, the State Administration of Press, Publication, Radio, Film, and Television, a powerful government agency, recommended in 2016 that the government take special management shares in media companies.[434] In April 2021, a state-backed firm acquired a one percent share of Beijing ByteDance Technology Co. (BBT); thus, it was able to send a board member to BBT.[435] Similarly, Weibo Corp. (which provides a Twitter-like service in China) sold 1 percent of its shares to a state investor and granted the state investor a seat on its board of directors.[436]

Jack Ma's speech on October 24, 2020, at the Bund Finance Summit in Shanghai, is illustrative.[437] His resentment of state interference was unmistakable when he commented that "[w]e cannot use the way to manage a

---

[428] Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Data Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021) 2021 Standing Comm. Nat'l People's Cong. Gaz. 1117, *translated in* Rogier Creemers & Graham Webster, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, DIGICHINA (Aug. 20, 2021), https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

[429] *Id*. art. 38.

[430] *Id*. art. 13.

[431] *Id*. art. 17.

[432] *Id*. arts. 33–37.

[433] Li Yuan, *Beijing Pushes for a Direct Hand in China's Big Tech Firms*, WALL ST. J. (Oct. 11, 2017, 7:27 PM), https://www.wsj.com/articles/beijing-pushes-for-a-direct-hand-in-chinas-big-tech-firms-15077-58314.

[434] Raymond Zhong & Sui-Lee Wee, *China Seeks Small Stakes in Online Companies, and More Power Over Them,* N.Y. TIMES, Oct. 14, 2017, at B3.

[435] *State Firm Takes Stake, Board Seat in ByteDance Unit*, S. CHINA MORNING POST, Aug. 18, 2021, at B1; Keith Zhai & Liza Lin, *Beijing Gets a Bigger Say at Internet-content Firms*, WALL ST. J., Aug. 18, 2021, at B1.

[436] Keith Zhai & Liza Lin, *id*., at B4.

[437] Kevin Xu, *Jack Ma's Bund Finance Summit Speech*, INTERCONNECTED (Oct. 24, 2020), https://interconnected.blog/jack-ma-bund-finance-summit-speech/.

railway station to manage an airport. We cannot use yesterday's way to manage the future."[438] However, distrust of privately operated tech firms was also brewing. A few months before Jack Ma's speech, a Data Security Act draft had been submitted to the national legislature for deliberation. In his statement to the NPC Standing Committee for the Data Security Act, in June 2020, Liu Junchen, Vice-Chair of the Legal Affairs Committee of the NPC Standing Committee, stated the reasons for enacting the Act:[439] first, Liu stated, the Party central leadership had realized that data had become a nation's "fundamental and strategic resource" (基础性战略资源), "no data security, no national security."[440] Second, Liu explained, "currently, multiple entities own data, processing them in complicated ways, thus security risks are high."[441] These statements revealed deep unease and skepticism among the top leadership about letting private companies hold large amounts of data crucial for the political status quo, despite all the measures taken.

In June 2021, the Ant Group was reportedly in talks with Chinese state-owned enterprises to create a credit-scoring company that would put the fintech giant's proprietary consumer data under regulators' purview.[442] Furthermore, in July 2021, the People's Bank of China (PBOC), China's central bank, "invited" Alibaba and Tencent to take part in developing the Digital Renminbi Yuan currency.[443] Again, the interest was clearly in Alibaba and Tencent's data. After all, it is property rights over the data that would give the authorities unchecked control—the ultimate goal of the surveillance state.

V. CONCLUSION

If the internet and social media is converting all political states into surveillance states, they are not monolithic. Rather, they can be divided into

---

[438] *Id.*

[439] Guanyu <Zhonghua Renmin Gongheguo Shuju Anquan Fa (Caoan)> de Shuoming–2020nian 6yue 28ri Zai Di Shisanjie Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Diershici Huiyi Shang (关于《中华人民共和国数据安全法（草案）》的说明——2020年6月28日在第十三届全国人民代表大会常务委员会第二十次会议上) [Statements on the Draft of the Data Security Act of the People's Republic of China–June 28, 2020 at the 13th National People's Congress Standing Committee 20th Session], STANDING COMM. OF THE NAT'L PEOPLE'S CONG. GAZ. 956 (2021).

[440] *Id*. On policy deliberation of this point in the internal circle, *see* NAT'L BUREAU OF ASIAN RSCH., CHINA'S DIGITAL AMBITIONS: A GLOBAL STRATEGY TO SUPPLANT THE LIBERAL ORDER 4 (Emily de La Bruyère et al. eds., 2022).

[441] Guanyu <Zhonghua Renmin Gongheguo Shuju Anquan Fa (Caoan)> de Shuoming–220nian 6yue 28ri Zai Dishisanjie Quanguo Renmin Daibiaodahui Changwu Weiyuanhui Diershici Huiyi Shang (关于《中华人民共和国数据安全法（草案）》的说明——2020年6月28日在第十三届全国人民代表大会常务委员会第二十次会议上) [Statements on the Draft of the Data Security Act of the People's Republic of China–June 28, 2020 at the 13th National People's Congress Standing Committee 20th Session], STANDING COMM. OF THE NAT'L PEOPLE'S CONG. GAZ. 956 (2021).

[442] Jing Yang & Lingling Wei, *China's President Xi Jinping Personally Scuttled Jack Ma's Ant IPO*, WALL ST. J., (Nov. 13, 2020, 12:56 PM), https://www.wsj.com/articles/china-president-xi-jinping-halted-jack-ma-ant-ipo-11605203556.

[443] Jing Yang, *Ant, Tencent Face Digital Yuan Dilemma,* WALL ST. J., Jul. 26, 2021, B1.

three classes, depending on their answer to the question of who owns data. In the United States, private companies such as Google and Facebook are the data collectors and the data they've collected are business records. In other words, the data are their property, "data collector's property" (DCP) theory defines privacy. The Fourth Amendment is interpreted as a guarantee of access to those data by the states. In the European Union, data subjects are considered co-owners of data. Therefore, the essential role of constitutional norms, interpreted by the CJEU, is to limit the access to data by the states. In illiberal states, data are increasingly collected by state-owned or state-controlled collectors, which means the states are becoming the primary data collectors themselves. Illiberal states insist the same—though more radical—DCP theories.

The division is a constitutional one, based on the central role that the constitution plays in the three classes of states. In the United States, DCP theories are used to justify the minimal reach of the Fourth Amendment and impoverish its jurisprudence. But that is the very point of DCP theories—to deny DSP. In the European Union, where it is acknowledged that data subjects have a say in controlling their data, then the constitutional norms are recognized and interpreted to provide guidance for legislatures in member countries. Therefore, the role of the constitutional norms is not to be minimal, but rather to be in a central position in curbing the powers of the states. Turkey and Russia show that in illiberal states, the constitutional courts are the willing agent of the state. In China, there is no constitutional court, not even a nominal one.[444]

The constitutional division, especially that between the United States and European Union, is perhaps shocking, just as the shared characteristics between the United States and illiberal states are unexpected. At its core, the constitutional division is about the function and nature of adjudication in courts. It is with this broad comparative context that the key characteristic modes of legal reasoning in the United States become visible. First, piecemeal rulings. The Fourth Amendment jurisprudence is more focused on specific technology than constitutional principles. The result is piecemeal rulings that provide little guidance to Congress. Second, binary judgments. Courts in the United States tend to rely on a series of conceptual dichotomies in these decisions. It is either your property or Google's; it is either reasonable or not to expect privacy; a warrant is either required or not. There are no in-betweens, no spectrums. Third, closely related to binary judgments in piecemeal rulings, there is no felt need to discuss procedural safeguards for data collection based on constitutional norms. It is the "mechanical jurisprudence" in the digital

[444] Keith Hand, *Constitutional Supervision in China after the 2018 Amendment of the Constitution: Refining the Narrative of Constitutional Supremacy in a Socialist Legal System*, 23 ASIAN-PAC. L. & POL'Y J. 137, 138 (2022).

world.[445] The result, however, is that the Supreme Court stopped functioning as a constitutional court.

[445] Roscoe Pound, *Mechanical Jurisprudence*, 8 COLUM. L. REV. 605 (1908).