TELEGRAPH, TELEPHONE AND THE INTERNET: THE MAKING OF THE SYMBIOTIC MODEL OF SURVEILLANCE STATES

Dongsheng Zang*
University of Washington School of Law

TABLE OF CONTENTS

* Associate Professor of Law, University of Washington School of Law. I would like to thank Xuan-Thao Nguyen, Jennifer S. Fan, Norman Page, Clark Lombardi, David Klein (Hamburg), David G. Litt and Daniel Foote (Tokyo) for the conversations or communications with me in the process of my research for this Article. Special thanks to Mr. Tom L. Aust, former student from my class at Keio University, for his research assistance. 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. From the summer of 2022 to the winter of 2023, I had the privilege and pleasure in working with Jesse W. Jordan of the *Arizona Journal of International and Comparative Law*. I wish to thank him for his help in shaping and improving the manuscript. Of course, all errors are mine.

I. INTRODUCTION

In the early 2000s, shortly before the September 11 attacks, Daniel J. Solove noted that computer databases in the United States were controlled by public as well as private bureaucracies.[1] In that sense, Solove argued, the "Big Brother" metaphor "fails to capture the most important dimension of the database problem."[2] In his 2008 Lockhart lecture, constitutional law scholar Jack M. Balkin argued that the United States has gradually transformed from a welfare and national security state to a National Surveillance State: "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."[3] Balkin considered this a "permanent feature of the governance."[4] Balkin noted, "much of the surveillance in the National Surveillance State will be conducted and analyzed by private parties,"[5] and that "the line between public and private modes of surveillance and security has blurred if not vanished."[6]

This Article aims to build on the insights from Daniel J. Solove and Jack M. Balkin in constructing a model of the surveillance state that is based on the public-private "partnership" in sharing data. I will call this the symbiotic model of the surveillance state. There is no doubt that the surveillance state has been investing and will continue to invest its own resources in building its own data—

---

1 Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002) [hereinafter Solove, *Privacy and Power*] (Symposium: Modern Studies in Privacy Law); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) [hereinafter Solove, THE DIGITAL PERSON]. The idea was soon shared by other scholars in the field, *see*, James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459 (2004) (The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901 (2008).

2 Solove, *Privacy and Power*, *supra* note 1, at 1399.

3 Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 5 (2008) [hereinafter Balkin, *Constitution in the National Surveillance State*]. Balkin believed that "The National Surveillance State grows naturally out of the Welfare State and the National Security State; it is their logical successor."; Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006) (Symposium: A New Constitutional Order) [hereinafter Balkin & Levinson].

4 Balkin, *Constitution in the National Surveillance State*, *supra* note 3, at 3; *see*, Orin S. Kerr, *The National Surveillance State: A Response to Balkin*, 93 MINN. L. REV. 2179 (2009); Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003).

5 Balkin, *Constitution in the National Surveillance State*, *supra* note 3, at 4.

6 *Id.* at 7.

the National Security Agency (NSA) being one prominent example.[7] The symbiotic model, however, claims that an increasing amount of data is collected and stored in private hands, and the surveillance state craves access to those data. After all, it is the private companies who create our favorite apps, gadgets, browsers, and platforms that collect data telling the most intimate aspects of our lives. In the words of Bruce Schneier, an acute observer of the tech world, what we face is a "very intimate form of surveillance."[8]

This Article proposes a symbiotic model of the surveillance state to provide a framework to understand the breadth and depth of surveillance in contemporary cyberspace in domestic law enforcement processes.[9] To achieve this goal, my analysis is built on insights from three dimensions: conceptual, historical, and comparative. In the conceptual dimension, this Article identifies three elements in the regulatory relations between data collectors and the regulatory state: (a) the very foundation for the control of data—property rights—which establishes and sets limits on constitutional constraints of the symbiotic relationship; (b) the doctrinal and statutory framework that forms the backbone of the symbiotic relationship; and (c) institutional dynamics in the symbiotic relationship. Bringing these elements together, this Article argues that, in the United States, digital platforms such as Google and Meta (Facebook) are data collectors, and their property claim over data is recognized by a judge-made rule called the third-party doctrine, which is interpreted from the Fourth Amendment.[10] This constitutional rule creates vast space and flexibility for the surveillance state to access the data by a convenient legal instrument called a subpoena. Data collectors, from time to time, resist the requests from surveillance states and fight the burden imposed on them; thus, the relationship is a dynamic one.

---

7 *See* Clapper v. Amnesty International USA, 568 U.S. 398 (2013) (NSA's wiretapping of telephones and interception of emails); *see also* Commonwealth v. Mora, 485 Mass. 360, 150 N.E.3d 297 (Mass. 2020); United States v. Jones, 565 U.S. 400 (2012); United States v. Caraher, 973 F.3d 57 (2nd Cir. 2020); United States v. Henderson, 906 F.3d 1109 (9th Cir. 2018).

8 BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 1 (2015).

9 Discussion of surveillance in this Article does not include the Foreign Intelligence Surveillance Act of 1978. Pub. L. No. 95-511, 92 Stat. 1783. Although, there is no doubt that this is a crucial part of the debate on surveillance states.

10 U.S. Const. amend. IV:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

For discussion of the third-party doctrine in interpretation of the Fourth Amendment, *infra*, Part IV, Section A.

However, one cannot have a clear picture of the surveillance state without considering aspects outside its own framework. To better understand the surveillance state, this Article seeks assistance from the second and third dimensions: the historical and comparative. Before the rise of the internet, Western Union, the most powerful telegraph company in the 1870s—1880s, and AT&T (the American Telephone and Telegraph Company), the most powerful telephone company up to the 1980s, were data collectors in their own times. They both faced requests for their data by a legal doctrine called subpoena *duces tecum*. Subpoena *duces tecum* is a Latin term for an order requiring the witness to appear in court and to bring specified documents, records, or other things,[11] and they fought them fiercely in court.[12] The historical dimension helps us track the doctrinal development of the legal rules. For example, subpoena *duces tecum*, which started as a grand jury's power, emerged as an administrative power in the 1920s,[13] was then consolidated in 1986 in the Stored Communication Act (SCA),[14] and finally expanded and entrenched for the internet age by the USA Patriot Act in 2001.[15] It was a gradual but persistent expansion in the reach of the surveillance state.

The third dimension—comparative—can help further our understanding of the surveillance state even more. In the times of the telegraph and telephone, Western Union and AT&T were both private companies; their counterparts in Europe (the British Telecom, for example) and East Asia (NTT, for Japan) were all state-owned and operated, until the privatization movements of the 1980s and 1990s.[16] Data-sharing between two agencies in the same bureaucracy, i.e., between the British police and the British Post Office for example, signifies very different dynamics from data-sharing between AT&T and the FBI, or Facebook and local law enforcement. The comparative law dimension shows that the symbiotic model, though not new to the United States, is a recent phenomenon for the rest of the world. It is a model that has spread from the United States and conquered the world, like the internet itself.

The symbiotic model, if successfully established, raises disturbing and soul-searching questions. Ultimately, the reach of the surveillance state is controlled by the highest judiciary which has the power and authority to interpret the Constitution. In 2006, Jack M. Balkin and Sanford Levinson warned us about the ideological movement of the United States Supreme Court towards

---

11 *Subpoena duces tecum*, *Black's Law Dictionary* (10th ed. 2014).

12 On Western Union and its litigation on subpoena duces tecum, *infra*, Part II, Section C; on AT&T and its efforts to fight wiretapping and pen registers, *infra*, Part III, Section B.

13 *Infra*, Part III, Section A.

14 Stored Communication Act ("SCA"), 18 U.S.C. §2701 et seq., enacted as Title II of the Electronic Communications Privacy Act of 1986, PL 99-508, Oct. 21, 1986, 100 Stat. 1848. For discussion of SCA and its expansion, *infra*, Part III, Section C.

15 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA Patriot Act") of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001). For discussion, *infra*, Part III, Section C.

16 *Infra*, Part III, Section D.

authoritarianism.[17] The Court's ruling in *Dobbs v. Jackson Women's Health Organization*[18] has seen it become a destructive force in American democracy. In post-*Roe* America, it seems that the surveillance state will only become further entrenched in the near future, as law enforcement would need digital platforms to provide information to control the crime of abortion.[19]

In the remainder of the Article, Part II will cover the first digital revolution—the era of the telegraph. It tracks the legal doctrine of subpoena *duces tecum* and Western Union's resistance to it, which led to a debate about whether telegrams should be privileged as mail, a major privacy debate in America prior to the Brandeis and Warren article.[20] Part III covers the history of another telecommunication revolution—the telephone—as well as the main player in this revolution—–AT&T. It tracks AT&T's resistance to wiretapping and third-party subpoenas, the Supreme Court's interpretation of the Fourth Amendment in this period, and how the SCA (enacted in 1986) became the very legal foundation for the era of the internet. Part IV of the Article surveys contemporary caselaw in the United States on the Fourth Amendment and key articles of SCA. It aims to show how data in the hands of digital platforms like Google and Facebook are channeled to the surveillance state on a regular basis, and often in secrecy. The analytical division of labor in this Article is deployed in the following ways: Parts II and III provide the historical dimension in the analysis, and Part IV is the description of the contemporary caselaw. In each of the three Parts, there is a comparative law section to provide the comparative dimension. The Article will conclude with some final remarks.

II. TELEGRAPH AND SUBPOENA DUCES TECUM

In 1838, Samuel F.B. Morse patented his first telegraphic device.[21] The first telegraph company was incorporated in 1845, in New Jersey. By the early 1850s, dozens of telegraph companies were set up.[22] After the Civil War, the

---

17 Balkin & Levinson, *supra* note 3.

18 Dobbs v. Jackson Women's Health Organization, 945 U.S. 265 (2022).Following the *Dobbs* ruling, a debate was immediately started on how to deal with the location-data regarding patients' visits to abortion clinics; *see* Patience Haggin, *Abortion Ruling Sparks Phone-Data Debate*, WALL ST. J., Aug. 8, 2022, at A7.

19 Bobby Allyn, *Privacy Advocates Fear Google Will be Used to Prosecute Abortion Seekers,* NPR (July 11, 2022), https://www.npr.org/2022/07/11/1110391316/google-data-abortion-prosecutions.

20 Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); *see* James H. Barron, *Warren and Brandies,* The Right to Privacy, 4 *Harv. L. Rev*. 193 (1890): *Demystifying a Landmark Citation*, 13 SUFFOLK U. L. REV. 875 (1979).

21 KENNETH SILVERMAN, LIGHTNING MAN: THE ACCURSED LIFE OF SAMUEL F.B. MORSE (New York, 2003).

22 Richard B. Du Boff, *Business Demand and the Development of the Telegraph in the United States, 1844-1860*, 54 BUS. HIST. REV. 459 (1980).

industry really took off. In 1877, Chief Justice Waite of the United States Supreme Court observed:

> The electric telegraph marks an epoch in the progress of time. In a little more than a quarter of a century it has changed the habits of business, and become one of the necessities of commerce. It is indispensable as a means of inter-communication, but especially is it so in commercial transactions.[23]

This first digital revolution was led by powerful private enterprise—Western Union.[24] It was also in this context that the issue of the Fourth Amendment right to privacy emerged,[25] approximately a decade before Louis Brandeis's famous article on the right to privacy in 1890.

A. Subpoena Duces Tecum in America

Before the American Civil War, it was established that a witness could be compelled to give evidence, so far as it did not subject himself to criminal prosecution.[26] In the Massachusetts case *Bull v. Loveland*,[27] a witness was issued a subpoena *duces tecum* to produce a promissory note and testify in court. Chief Justice Shaw on the Supreme Judicial Court of Massachusetts said:

> It has been decided, though it was formerly doubted, that a subpoena *duces tecum* is a writ of compulsory obligation, which the court has power to issue, and which the witness is bound to obey, and which will be enforced by proper process to compel the production of the paper, when the witness has no lawful or reasonable excuse for withholding it.[28]

---

23 Pensacola Telegraph Co. v. Western Union Telegraph Co., 96 U.S. 1, 9 (1877).

24 JOSHUA D. WOLFF, WESTERN UNION AND THE CREATION OF THE AMERICAN CORPORATE ORDER, 1845-1893 (Cambridge 2013); *see*, CAROLYN MARVIN, WHEN OLD TECHNOLOGIES WERE NEW: THINKING ABOUT ELECTRIC COMMUNICATION IN THE LATE NINETEENTH CENTURY (Oxford 1989); ROBERT L. THOMPSON, WIRING A CONTINENT: THE HISTORY OF THE TELEGRAPH INDUSTRY IN THE UNITED STATES, 1832-1866 (Princeton, 1947).

25 Thomas Jepsen, *"A New Business in the World": The Telegraph, Privacy, and the U.S. Constitution in the Nineteenth Century*, 59 TECH. & CULTURE 95 (2018).

26 *See* Taney v. Kemp, 4 Harris & Johnson 348 (Md. 1818) (ruling a witness could be compelled to given evidence); *see also* Baird v. Cochran, 4 Sergeant & Rawle 397 (Pa. 1818); Stoddert v. Manning, 2 Harris & Gill 147, 158 (Md. 1828) ("[s]ince the case of Taney v. Kemp . . . it may be laid down as a rule of evidence, that no person shall be exempted from giving testimony on the ground that his answer may affect his interest."

27 Bull v. Loveland, 10 Pickering 9 (Mass. 1830).

28 *Id.* at 14.

In 1842, Simon Greenleaf observed that this was the function of the writ of subpoena *duces tecum* for the production of private papers.[29] States adopted policy to facilitate the industry, and part of this policy was non-disclosure rules for telegraph operators.[30] The state of New York, for example, passed a law in April 1850 that imposed a misdemeanor on any clerk, operator, or messenger who willfully divulged the contents of telegrams.[31] Similarly, in April 1851, Pennsylvania made it unlawful to disclose telegrams "without the consent or direction of either the party sending or receiving" the dispatch.[32] The Pennsylvania law declared:

> all dispatches which may be filed at any office in this commonwealth for transmission to any point, shall be so transmitted without being made public, or their purport in any manner divulged at any intermediate point on any pretense whatever, and in all respects the same inviolable secrecy, safe keeping, and conveyance shall be maintained by the officers and agents employed upon the several telegraph lines of this commonwealth . . . .[33]

In June 1851, two months after Pennsylvania passed this law, *Henisler v. Freedman* was brought before the Court of Common Pleas.[34] Here, a manager of a telegraph company was issued a subpoena as a witness in a case in which the telegraph company was not a party. The subpoena required the manager to testify about a certain telegraph dispatch and produce it. The manager admitted that he had the dispatch in his possession but claimed that he was exempt from the obligation by virtue of the new act. Judge Edward King, president of the Court of Common Pleas, rejected the claim that telegraphs were privileged communications: "[f]or the result of the principle contended for is, that the seal of secrecy is placed on all telegraphic communications, as well as in courts of justice as elsewhere, and that they are to be classed with privileged communications, such as those between husband and wife, counsel and client."[35] Judge King pointed out, "[t]he real intent

---

29 SIMON GREENLEAF, A TREATISE ON THE LAW OF EVIDENCE §558 and §559 (1842); *see* ESEK COWEN, A TREATISE ON THE CIVIL JURISDICTION OF A JUSTICE OF THE PEACE IN THE STATE OF NEW YORK 518 (1821) (discussing the procedural aspects of subpoena *duces tecum*).

30 Tomas Nonnenmacher, *State Promotion and Regulation of the Telegraph Industry, 1845-1860*, 61 J. ECON. HIST. 19 (2001); H. H. Goldin, *Governmental Policy and the Domestic Telegraph Industry* 7 J. ECON. HIST. 53 (1947); WILLIAM L. SCOTT & MILTON P. JARNAGIN, *Penalties and Indictment by Statute in Relation of Messages, in* A TREATISE UPON THE LAW OF TELEGRAPHS 406-09 (1868).

31 1850 N.Y. Laws 739.

32 Section VII of an Act passed on Apr. 14, 1851, Pamph. L. 616, GENERAL LAWS OF PENNSYLVANIA 1140 (James Dunlop ed. 1853).

33 *Id.*

34 Henisler v. Freedman, 2 Parsons 274 (1851).

35 *Id.* at 277.

and object of this law, was to prevent the betrayal of private affairs, communicated through the telegraph by those connected with it, for the promotion of private gain, or the gratification of idle gossip."[36] The judge reasoned that, "in using the phrase 'unlawfully expose another's business or acts,' the Legislature certain show, that they did not consider all exposures of another's business or acts . . . to be 'unlawful.'"[37] Thus, the judge concluded:

> If we are asked what are lawful exposures of business or acts, communicated through telegraph, the answer would seem to be, exposure made in courts, in the course of the administration of public justice; or exposures made to the public authorities for the sole and bona fide motive of preventing crime, or leading to its detection or punishment.[38]

During the 1860s, the *Henisler* ruling was recognized as the general rule that telegrams were not privileged communications.[39] As the telegraph gained popularity in business, telegraphic messages were increasingly used as evidence in court.[40] However, the question of which communications were privileged remained unclear as a matter of constitutional principle, especially when Judge Thomas M. Cooley, a respected scholar sitting on the bench of the Michigan Supreme Court,[41] joined the debate shortly after the Civil War.

---

36 *Id.*

37 *Id.* at 277–78.

38 *Id.* at 278.

39 WILLIAM L. SCOTT & MILTON P. JARNAGIN, A TREATISE UPON THE LAW OF TELEGRAPHS §§375-78 (1868) (discussing the ruling of *Henisler*); Charles Allen, TELEGRAPH CASES DECIDED IN THE COURTS OF AMERICA, GREAT BRITAIN, AND IRELAND 1 (Charles Allen ed. 1873)(Charles Allen served as Attorney General of the Commonwealth of Massachusetts from 1861 to 1872, and then Associate Justice of the Supreme Judicial Court of Massachusetts from 1881 to 1898).

40 For example, in a contract dispute, the telegraph operator testified there was a delivery of telegraph. The court: holding that a contract made through the medium of a telegraph is enforceable: "It is not expected, when men contract by telegraph, that they are afterwards to be bound or not, as their passions or interests may dictate. Such contracts must be regarded as binding and obligatory as if made in the ordinary way." Taylor v. Steamboat Robert Campbell, 20 Mo. 254, 259 (Mo. 1855); Morris Wolf, *Liability of Telegraph Companies*, 42 AM. L. REG. 715 (1903).

41 *See* Paul D. Carrington, *The Constitutional Law Scholarship of Thomas McIntyre Cooley*, 41 AM. J. LEGAL HIST. 368 (1997); William J. Fleener, Jr., *Thomas McIntyre Cooley: Michigan's Most Influential Lawyer*, 79 MICH. B.J. 208 (2000); Phillip S. Paludan, *Law and the Failure of Reconstruction: The Case of Thomas Cooley*, 33 J. HIST. OF IDEAS 597 (Dec. 1972).

B. Judge Cooley and Telegrams

In his influential treatise, *Constitutional Limitations*, Judge Thomas M. Cooley elaborated on constitutional constraints on unreasonable searches and seizures under the Fourth Amendment.[42] Judge Cooley stated that it is not "allowable to invade one's privacy for the purpose of obtaining evidence against him."[43] This was followed by a footnote stating that "[t]he fourth amendment to the Constitution of the United States, found also in many state constitutions, would clearly preclude the seizure of one's papers in order to obtain evidence against him."[44]

Judge Cooley went even further by making some comments on liberty: "The importance of public confidence in the inviolability of correspondence, through the post-office, cannot well be overrated, and the proposition to permit letters to be opened at the discretion of a ministerial officer, would be met with general indignation."[45] In making this comment, he anticipated *Ex parte Jackson*,[46] where ten years later the United States Supreme Court declared that the secrecy of letters was protected by the Constitution. Judge Cooley extended this principle to telegraph: "[t]he same may be said of private correspondence by telegraph; the public are not entitled to it for any purpose . . . In either case, it would be equivalent to an unlawful and unjustifiable seizure of his papers, — such an 'unreasonable seizure' as is directly condemned by the Constitution."[47]

Two years after the publication of *Constitutional Limitation*, the Supreme Court of Maine decided *State v. Litchfield*.[48] In this case, defendant Alden

---

42 THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS 299-308 (1868).

43 *Id.* at 305.

44 *Id.* at 305-06. *see also* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 778 (1994) (discussing Judge Cooley's understanding of warrant in the Fourth Amendment).

45 *Id.* at 307.

46 Ex parte Jackson, 96 U.S. 727, 733 (1877) (writing for a unanimous court, Justice Field announced: "Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."); Historian Anuj C. Desai argued that "*Ex parte Jackson* was not decided solely on the abstract principle that courts should guard communications privacy. The *Ex parte Jackson* Court applied that principle to a unique medium to which Congress itself had long since applied the very same principle. Thus, the Court's first articulation of what one might view as a bold Fourth Amendment principle was actually tethered to a very specific institutional context." Anuj C. Desai, *Wiretapping before the Wires: The Post Office and the Rebirth of Communications Privacy*, 60 STAN. L. REV. 553, 583-84 (2007); s*ee also* Anuj C. Desai, *The Transformation of Statutes into Constitutional Law: How Early Post Office Policy Shaped Modern First Amendment Doctrine*, 58 HASTINGS L.J. 671 (2006-2007).

47 THOMAS M. COOLEY, *supra* note 42, at 308.

48 State v. Litchfield, 58 Me. 267 (1870).

Litchfield was indicted in a larceny case. During trial, the State offered to prove contents of a telegram deemed material to the case. Defendant's counsel objected on the ground that the telegram was privileged communication.[49] The question for the Court was whether a telegraph operator can be compelled to testify to the contents of a telegraphic message. A unanimous Maine Supreme Court rejected the contention in a straight way: any "written message, or its contents, after due notice to produce the original, . . . would be received in evidence."[50] Telegraphic communications, the Court stated, cannot be deemed "any more confidential than any other communications."[51] Court centered on its claim of public interest: "[t]he interests of the public demand that resort should be had to all available testimony . . . the telegraphic operator, as such, can claim no exemption from interrogation."[52]

The second case was *United States v. Babcock*.[53] In January 1876, William Orton, president of Western Union, was served subpoena *duces tecum* by the United States in a criminal case to which Western Union was not a party. The subpoena required Orton to produce telegrams. Orton, represented by a prominent St. Louis, Missouri attorney, Mr. Henry Hitchcock,[54] filed a motion to set aside the subpoena.[55] Hitchcock's objection to the subpoena was that it had been "improvidently issued."[56] It seemed that Hitchcock did not follow Judge Cooley in claiming that telegrams were privileged. Judge Dillon took note of this and recorded that "[n]o objection is made on the ground that these [telegraphic] messages are privileged, confidential communications,"[57] so the court did not rule on this issue. Rather, the court focused on the question of whether the subpoena was sufficiently certain in describing the dispatches required.[58] Ultimately, it denied the motion and compelled Western Union to produce the telegrams.

In 1879, Judge Cooley published an article titled "Inviolability of Telegraphic Correspondence" in the *American Law Register*.[59] Cooley argued that "secrecy tends to the promotion of public and family confidence and encourages a most valuable feeling of security in free intercommunication between all classes of

---

49 *Id.* at 268.

50 *Id.* at 269.

51 *Id.*

52 *Id.* at 270.

53 United States v. Babcock, 24 F. Cas. 908 (C.C.E.D. Mo. 1876) (No. 14,484), 3 Dill. 566 (1876).

54 ST. LOUIS CNTY. BAR ASSOC., HENRY HITCHCOCK 1829-1902, at 8 (St. Louis, Goftschalk Print. Co.) (1902); WALTER BARLOW STEVENS, CENTRAL HISTORY OF MISSOURI: MISSOURI THE CENTER STATE 1821-1915 (1915).

55 Babcock, 24 F. Cas.at 908.

56 *Id.*

57 *Id.*

58 *Id.* at 909.

59 *Inviolability of Telegraphic Correspondence*, 18 AM. L. REG. 65 (1879). (The article was not marked, but the authorship is 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*, REPORT OF THE SECOND ANNUAL MEETING OF THE AMERICAN BAR ASSOCIATION 93, 103 (1879); DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 38 (1978).

community."[60] Cooley even warned that "the American people would never tolerate official surveillance of their private and business correspondence."[61]

C. Western Union and Subpoena Duces Tecum

Western Union was involved in some important *duces tecum* disputes. Western Union was founded in New York in 1851,[62] and experienced phenomenal growth over the following twenty years. By 1871, Western Union owned more than two-thirds of the telegraph wire in the United States and transmitted ninety percent of all the messages.[63] Western Union had an optimistic view in regarding itself as an agent of peace and universal communication.[64]

The first subpoena *duces tecum* case involving Western Union was *United States v. Babcock* (1876),[65] discussed earlier. The issue came up again in December 1876 when the United States House of Representatives issued a subpoena *duces tecum* to Edmund W. Barnes, manager of Western Union in New Orleans, Louisiana,[66] to appear before a House special committee and produce "all telegrams" sent and received by people in relation to an investigation of election.[67] Under the instruction of William Orton, Barnes appeared in front of the committee but refused to produce the telegrams. Barnes was thus found in contempt on January 12, 1877, by the House Judiciary Committee.[68]

A similar incident happened in St. Louis in April 1879,[69] when E. A. Brown, a local manager of Western Union at St. Louis was served a subpoena *duces tecum* by the St. Louis Criminal Court, which required him to testify before the grand jury and produce telegrams. The subpoena demanded "any and all telegraphic dispatches or messages, or copies of the same, now in the office of the Western Union Telegraph Company, of which you are manager, and which

---

60 *Id.* at 70.

61 *Id.* at 72.

62 At its founding, its name was New York and Mississippi Valley Printing Telegraph Company, and the name Western Union Telegraph Company was adopted in 1856 after merger with Erie and Michigan Telegraph Company, *see* JAMES D. REID, THE TELEGRAPH IN AMERICA: ITS FOUNDERS PROMOTERS AND NOTED MEN 464-67 (New York, 1879); *See also* JOSHUA D. WOLFF, WESTERN UNION AND THE CREATION OF THE AMERICAN CORPORATE ORDER, 1845-1893 (Cambridge 2013).

63 WOLFF, *supra* note 62; Richard T. Ely, *The Telegraph Monopoly*, 149 NORTH AM. REV. 44 (1889); Richard B. du Boff, *The Telegraph in Nineteenth-Century America: Technology and Monopoly*, 26 COMP. STUD. SOC. & HIST. 571 (1984).

64 Richard R. John, *Private Enterprise, Public Good?: Communications Deregulation as a National Political Issue, 1839–1851*, in BEYOND THE FOUNDERS: NEW APPROACHES TO THE POLITICAL HISTORY OF THE EARLY AMERICAN REPUBLIC 328-54 (Jeffrey L. Pasley, Andrew W. Robertson & David Waldstreicher eds. 2004).

65 Babcock, 24 F. Cas. at 908

66 JAMES D. REID, *supra* note 62, at 841.

67 5 CONG. REC. 352 (Dec. 21, 1876).

68 5 Cong. Rec. 602 (Jan. 12, 1877) (44th Cong. 2d sess.).

69 Ex parte Brown, 7 Mo. App. 484 (St. Louis Ct. of App., 1879).

dispatches and messages are now in your possession and under your control."[70] Brown was found in contempt when he refused to produce the telegrams and subsequently appealed to the St. Louis Court of Appeals on habeas corpus. Judge Hayden, writing for the majority, found that well-settled rules on writ of subpoena *duces tecum* applied to telegraphs, and "there is no peculiarity in the telegraphic messages, as such, which exempts them or their contents from the process of the courts."[71] The appellate court thus affirmed the lower court's decision.

Judge Lewis, however, dissented and wrote an elaborate critique of the majority opinion.[72] For Judge Lewis, the "*subpoena duces tecum* in this case bears upon its face the odious features of the general warrant which the framers of our government intended to banish from American jurisprudence."[73] Thus, the majority's failure to require a particular description in the subpoena was "in utter disregard of recognized essentials of the subpoena deuces tecum, and in violation of the constitutional guaranty against 'unreasonable searches and seizures.'"[74] Judge Lewis believed that the subpoena "invades the domain of lawful privacy."[75]

In August 1879, Henry Hitchcock read his paper, "The Inviolability of Telegrams," at the Annual Meeting of the American Bar Association.[76] Apparently prompted by recent events surrounding Western Union and Judge Cooley's article with similar title,[77] Hitchcock shared Judge Lewis's dissenting opinion and integrated it with those of Judge Cooley by resorting to the Fourth Amendment. Similarly, in December 1879, John L. Thompson, a prominent lawyer from Chicago, testified as counsel for Western Union at the United States Senate Committee on Privileges and Elections.[78] On the other hand, Francis Wharton, arguing against privilege, warned that granting privilege meant to put "in the hands of telegraph companies a power perilous to public welfare."[79]

The case eventually went to the Supreme Court of Missouri.[80] In a unanimous decision, the Court adopted Hitchcock's article and Judge Lewis'

---

70 *Id.* at 495-86.

71 *Id.* at 493.

72 *Id.*

73 *Id.* at 500.

74 Brown, 7 Mo. App. at 495.

75 *Id.* at 496.

76 Hitchcock, *Inviolability*, *supra* note 59. (Hitchcock's article was subsequently re-published in *Southern Law Review*); *see* Henry Hitchcock, *The Inviolability of Telegrams*, 5 SOUTH. L. REV. 473 (1879)(all reference to Hitchcock's article is page numbers in the *Annual Report of the American Bar Association*).

77 Hitchcock, *supra* note 59.

78 U.S. CONG., REPORTS OF COMMITTEES OF THE SENATE OF THE UNITED STATES FOR THE FIRST AND SECOND SESSIONS OF THE FORTY-SIXTH CONGRESS, 1879-'80 (1880).

79 Francis Wharton, *Telegraph Privilege*, 13 CENT. L. J. 42, 43 (1880). *see also* FRANCIS WHARTON, A TREATISE ON THE LAW OF EVIDENCE IN CRIMINAL ISSUES §506 (8th ed. 1880).

80 Brown, 72 Mo. 83..

dissenting opinion,[81] and declared that "[t]elegraphic messages are not privileged communications."[82] It explicitly rejected the analogy of telegrams and mails: "There is no such analogy between the transmissions by mail, and their transmission by telegraph . . . ."[83] However, the Court found the Missouri Bill of Rights prohibited unreasonable searches and seizures. By issuing a broad subpoena *duces tecum* without having specified "date, title, substance, or subject matter,"[84] the Court reasoned, it became an "indiscriminate search," thus contrary to the Bill of Rights. Therefore, the Court ordered petitioner Brown to be discharged from custody.[85]

The Supreme Court of Missouri set the standard in *Ex parte Jaynes*.[86] In *Ex parte Jaynes*, the Supreme Court of California set aside a subpoena *duces tecum* issued to the Western Union, which required production of all telegrams transmitted to or from named places between specified dates by a large number of persons. Similarly, in *United States v. Hunter*,[87] a federal court for the Northern District of Mississippi ruled to quash the subpoena because it did not contain the required particularity information. There was no question, for the court, that "[w]hen such a subpoena is served upon the person having the possession of the telegram, it is his duty to appear before the grand jury or court and produce the telegram."[88] If the subpoena did not have these problems, courts enforced them without question. In *Woods & Bradley v. Frank Miller & Co.*,[89] a telegraph operator in Iowa was subpoenaed to testify and produce the telegrams between the parties to a contract dispute. The operator objected, the trial court overruled the objection, and the telegrams were introduced as evidence. The Supreme Court of Iowa held that the trial court did not err in overruling the objection. In *Wertheim v. Continental Railway & Trust Co.*,[90] the president and secretary of North River Construction Company—a non-party to the dispute—was served a subpoena *duces tecum*, to produce books and papers of the corporation in a suit. *People ex rel. Sabold v. Webb*,[91] a decision by the Supreme Court of New York, answered the question of whether the New York Assembly had the power to subpoena a manager of Western Union to produce telegrams as evidence in a special investigation.[92] While the issue

---

81 *Id.* at 96-97 ("An interesting article on the questions discussed in this opinion, read by Henry Hitchcock, Esq. of the St. Louis bar . . . has been of great service to us in our investigations, and is a valuable contribution on the subject.").

82 *Id.* at 90.

83 *Id.* at 91.

84 *Id.* at 94.

85 *Brown*, 72 Mo. at 97..

86 Ex parte Jaynes, 70 Cal. 638, 12 P. 117 (1886).

87 United States v. Hunter, 15 Fed. 712 (N.D. Mis. 1882).

88 *Id.* at 715.

89 Woods & Bradley v. Frank Miller & Co., 55 Iowa 168, 7 N.W. 484 (1880).

90 Wertheim v. Cont. R.& Tr. Co., 15 F. 716 (C. C. S.D.N.Y. 1883).

91 People ex rel. Sabold v. Webb, 5 N.Y.S. 855, (Sup.Ct. 1889).

92 N.Y. LEG. ASSEMB., DOCUMENTS OF THE ASSEMBLY OF THE STATE OF NEW YORK (1889).

was "argued at great length, and with marked ability,"[93] Judge Mayham, writing for a unanimous court, concluded that ". . . upon principle and authority, that telegrams, as such, are not privileged; that they are clearly distinguishable from communications sent by mail while in transit . . . ."[94] Although, the judge ultimately concluded that he did not need to rule on that question.

Despite Cooley coming into preeminence as an authority on the Constitution in the 1880s,[95] his theory and perspective remained unmentioned in any of the above discussed cases.[96] Thus, in 1885, Morris Gray, in his influential treatise on telegram, concluded that "[t]he view that telegraph messages in the hands of telegraph companies are entitled, as such, to protection from disclosure in courts of justice cannot be supported."[97]

D. Comparative Perspective

In Europe, the telegraph industry was a state monopoly. In the Netherlands, the State Telegraph Service was established in 1852.[98] In Germany, Carl Steinheil, and Werner Siemens relied on state funding to build and experiment with Germany's early telegraph lines.[99] Siemens set up his business in 1847, Siemens & Halske, relied on state contracts. According to historian Jean-Michel Johnston, "[b]y 1849, the state had established its control over telegraph networks across Germany."[100] In Great Britain, telegraph was started by private entrepreneurs in 1838[101] but was brought to state ownership and control by the British Post Office in 1870.[102] In Japan, the first telegraph line—between Tokyo and Yokohama—was erected in

---

93 Webb, 5 N.Y.S. at 861.

94 *Id.* at 857.

95 *See*, A RECORD OF THE COMMEMORATION, NOVEMBER FIFTH TO EIGHT, 1886, ON THE TWO HUNDRED AND FIFTIETH ANNIVERSARY OF THE FOUNDING OF HARVARD COLLEGE (Harvard University 1887) (In 1886, Judge Cooley was awarded an honorary doctorate by Harvard Law School when Harvard University celebrated her 250th anniversary); Paul D. Carrington, *Law as "The Common Thoughts of Men": The Law-Teaching and Judging of Thomas McIntyre Cooley*, 49 STAN. L. REV. 495 (Feb. 1997) (noting, "At this time, Cooley was the most respected lawyer in America and among the most widely respected persons in American public life.").

96 *In re Storror*, 63 F. 564 (N.D. Calif. 1894) (ruling in a sympathetic manner while also disagreeing with Judge Cooley).

97 MORRIS GRAY, A TREATISE ON COMMUNICATION BY TELEGRAM §121 (Boston, 1885).

98 Mila Davids, *The Relationship Between the State Enterprise for Postal, Telegraph and Telephone Services and the State in the Netherlands in Historical Perspective*, 24 BUS. & ECON. HIST. 194, 196 (Fall 1995, No.1).

99 JEAN-MICHEL JOHNSTON, NETWORKS OF MODERNITY: GERMANY IN THE AGE OF THE TELEGRAPH, 1830-1880 (Oxford, 2021).

100 *Id.* at 78.

101 SIMONE FARI, VICTORIAN TELEGRAPHY BEFORE NATIONALIZATION (2015).

102 HUGO RICHARD MEYER, THE BRITISH STATE TELEGRAPHS: A STUDY OF THE PROBLEM OF A LARGE BODY OF CIVIL SERVANTS IN A DEMOCRACY 75 (1907).

December 1869,[103] the second year of the Meiji Restoration. In September 1872, the Meiji government decided that no private telegraphs should be permitted. In May 1885, the Japanese Telegraph Code declared telegraphs a monopoly of the government.[104]

Under English law, subpoena *duces tecum* was available for grand jury and it became clear by the 1880s that telegraphic messages were not privileged. Prior to the arrival of telegraph, subpoena *duces tecum* had long been established in English law.[105] However, there was a dark side of state-control. For a long time in British history, the Home Secretary had the power to open letters; and that power was extended to telegrams.[106] This had been kept secret until June 1844, when a petition was brought to the House of Commons[107] by four gentlemen alleging their sealed letters had been opened at the Post Office. A secret committee was quickly appointed and investigated the matter.[108] The report revealed that a statute from the reign of Queen Anne (1710) had authorized detaining and opening of letters at the Post Office when authorized by an "express warrant" from one of the principal secretaries of state.[109] While the secret committee noted "strong moral feeling" against such a practice, it did not recommend abolishing it in the 1844 report, for fear that ability to control crime would be "greatly diminished."[110]

The development in Continental Europe was similar. During the 1848 Revolutions, the Frankfurt National Assembly was seriously engaged in debates on

---

103 J. Morris, *Telegraphs in Japan*, 10 JOURNAL OF THE SOCIETY OF TELEGRAPH ENGINEERS AND OF ELECTRICIANS 127 (1881, No.36); SHINJIRO MAYEDA, OUTLINES OF THE HISTORY OF TELEGRAPHS IN JAPAN 27 (1892).

104 MAYEDA, *supra* note 103, at 26; *contra* ERIK BAARK, LIGHTNING WIRES: THE TELEGRAPH AND CHINA'S TECHNOLOGICAL MODERNIZATION, 1860-1890 (1997 Volume 1), at 72-74, 81. (Chinese Qing officials resisting the idea of telegraph during the 1860s and the first telegraph line was laid by Danish company Great Northern in 1870).

105 Borough of Harwich, 3 O'Malley & Hardcastle 61 (1880) (remedying the confusion caused by Borough of Stroud, 2 O'Malley & Hardcastle 107 (Apr. 1874) case. The rule was similar throughout the British Empire. In Ireland, cases included In re Thomas J. Smith, 7 L. R. Ir. 286 (Court of Bankruptcy, 1881), Colgan v. Quinn, 17 Ir. L. T. Rep. (1883). In Australia, In the Matter of Patrick O'Brien, 13 S.A. Law Rep. 79 (Sup. Ct. South Australia, 1879). In Canada, Dwight v. Macklam, 15 Ontario Reports 148 (1888). There were still intensive interests in the question of privilege in telegraphic messages, but the conclusion seemed universal in denying it. *See Privilege on the Ground of Public Policy*, 4 AUST. L. T. xii (Jul. 22, 1882, No.69), *The Inviolability of Telegrams*, 14 IRI. L. T. 281 (Jun. 1880)).

106 SIR WILLIAM R. ANSON, THE LAW AND CUSTOM OF THE CONSTITUTION 233 (2d ed. 1896).

107 *Opening Letters—Post Office* (House of Commons, June 14, 1844), 75 HANSARD'S PARLIAMENTARY DEBATES col. 892 (1844).

108 *The Report from the Secret Committee on the Post-Office* (Aug. 5, 1844), in 14 PARLIAMENTARY PAPERS 582 (1844)[hereinafter *Secret Committee*] (finding that the annual average in Great Britain of such warrants did not exceed 6).

109 An Act for Establishing a General Post Office for All Her Majesty's Dominions, and for Settling a Weekly Sum out of the Revenues Thereof, for the Service of the War, and Other Her Majesty's Occasions, 9 Queen Anne c. 10, Sec. 40.

110 Secret Committee, *supra* note 108, at 601.

constitutional protection of privacy in letters.[111] The influence of the 1848 Revolution led eventually to a series of legislations in the 1870s, including the 1877 German Code of Criminal Procedure.[112] This Code, though highly regarded as progress in reforming German criminal procedure, also permitted interception of letters and telegrams addressed to the accused.[113]

If the telegraph was the first digital revolution in recent history, privacy did not win this legal battle in the United States, Great Britain, Continental Europe, or elsewhere. However, the fact that Western Union was a private company that was not under direct control of the government meant there was a different dynamic to the question of privacy in the United States. It was more open and conducted through the language of constitutional norms than the rest of the world. In that sense, the United States had a good start on the journey towards becoming a surveillance state.

III. TELEPHONE AND THE THIRD-PARTY SUBPOENA

The telephone was invented in 1876.[114] By the mid-1880s, telephones had become so widely used that a physician would lose significant business if he did not own one.[115] In 1885, the American Telephone and Telegraph Company, better known as AT&T, was incorporated. In subsequent years, AT&T would become a dominant power in the telecommunication market until its breakup in 1984. At the time of AT&T's breakup, multiple players were active in the telecommunication service market. To add further perspective on the market in 1984, computers had become widely available, and popularity of the cellular phone was on the rise. It was in this context that the Stored Communication Act (SCA) passed in 1986.[116] The SCA became the foundation for the symbiotic model. Until 1985, telephone

---

111 Thomas J. Snyder, *Developing Privacy Rights in Nineteenth-Century Germany: A Choice between Dignity and Liberty*, 58 AM. J. LEGAL HIST. 188 (2018); *Verfassung für den Preußischen Staat* [Constitution] Jan. 31,1850, art. 33 (Prus.) (guaranteeing privacy of mail).

112 H. A. D. Phillips, *German Code of Criminal Procedure*, 10 L. Q. REV. 16 (1894); B. L. Mosely, *German Criminal Courts and Procedure*, 10 LAW MAG. & L. REV. 5th ser. 369 (1885); Ronnie Bloemberg, *The Development of the German Criminal Law of Evidence between 1750 and 1870: From the System of Legal Proofs to the Freie Beweiswurdigung - Part 1*, 9 J. EUR. HIST. L. 2 (2018); *The Development of the German Criminal Law of Evidence between 1750 and 1870: From the System of Legal Proofs to the Freie Beweiswurdigung - Part 2*, 9 J. EUR. HIST. L. 2 (2018).

113 H. A. D. Phillips, *id.* at 26; B. L. Mosely, *id.* at 387; *see* ELAINE GLOVKA SPENCER, POLICE AND THE SOCIAL ORDER IN GERMAN CITIES: THE DÜSSELDORF DISTRICT, 1848-1914 80 (1992) (finding that police called upon post officials to open the letters for them—while the postal director in Essen chose to comply, Düsseldorf refused).

114 *See* ALVIN FAY HARLOW, OLD WIRES AND NEW WAVES: THE HISTORY OF THE TELEGRAPH, TELEPHONE, AND WIRELESS 356-60 (1936) (Alexander Graham Bell submitted his application for patent on February 14, 1876 and was granted the patent on March 7).

115 *Id.* at 394.

116 *See infra* Part III, Section C.

was still a state-owned business in Great Britain, Continental Europe, and Japan.[117] With rising concerns of privacy at home, each initially tried a different regulatory approach in the 1970s, but all of them soon decided to embrace the American model.

A. Proliferation of Third-Party Subpoenas

During the 1920s, while grand juries continued to issue subpoena *duces tecum* to telegraph operators,[118] subpoenas were also increasingly issued by administrative agencies. 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."[119] In *Brownson v. United States*, G. W. Brownson, superintendent of the Western Union in Kansas City, Missouri, was held in county jail for failing to produce telegraphs required by a subpoena, issued by the Commission of Internal Revenue.[120] Based on the Revenue Act of 1918,[121] the Eighth Circuit reached its conclusion that the subpoena was enforceable.[122] In this seemingly routine decision, however, the Eighth Circuit was totally conscious of what was new in this case—that it was not a subpoena issued by a grand jury, but by a federal administrative agency. The Eighth Circuit was quite explicit about this point in its ruling:

---

117 A. N. HOLCOMBE, PUBLIC OWNERSHIP OF TELEPHONES ON THE CONTINENT OF EUROPE (1911); HERBERT LAWS WEBB, THE DEVELOPMENT OF THE TELEPHONE IN EUROPE (1911); HUGO RICHARD MEYER, PUBLIC OWNERSHIP AND THE TELEPHONE IN GREAT BRITAIN RESTRICTION OF THE INDUSTRY BY THE STATE AND THE MUNICIPALITIES (1907).

118 Ex parte Gould, 60 Tex. Cr. 442,132 S.W. 364 (Crim. App. 1910).

119 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).

120 Brownson v. United States, 32 F.2d 844 (8th Cir. 1929).

121 Revenue Act of 1918, 26 U.S.C. §1247, repealed, Pub. L. 108-357, Title IV, §413(a)(2), (3), Oct. 22, 2004, 118 Stat. 1506. Initially, Revenue Act of 1918, 40 Stat. 1057, Section 1305 provides:

> The Commissioner [of Internal Revenue], 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, or the attendance of any other person having knowledge in the premises, and may take his testimony with reference to the matter required by law to be included in such return, with power to administer oaths to such person or persons.

122 Brownson v. United States, 32 F.2d 844, 848 (8th Cir. 1929).

> We think that the power granted to the Commissioner of Internal Revenue by the statutes above quoted to require the attendance of witnesses and the production of books and papers in matters properly under investigation by him is similar to the power vested by analogous statutes in federal grand juries to perform similar acts . . . .[123]

Among the authorities that the Eighth Circuit relied upon was *United States v. First National Bank of Mobile*,[124] where a federal district court ruled that the Bureau of Internal Revenue, based on a similar statute, had the right to request a commercial bank to produce information of a customer and his wife. In subsequent years, especially in the 1950s, federal courts repeatedly upheld administrative subpoenas issued by IRS to banks, accountants, lawyers, and even hospitals for information of either their customers, clients, or patients.[125] Similarly, the Securities Act of 1933 gave power to the Securities Exchange Commission (SEC),[126] the Fair Labor Standards Act 1934 to the Administrator of the Wage and Hour Division.[127] Similarly, the Communication Act of 1934 granted broad authority to the Federal

---

123 *Id*. at 848 (This point was confirmed by the United States Supreme Court in 1945 in a case on the Labor Administrator's investigative function under the Fair Labor Standards Act, the Court stated "in search out violations with a view to securing enforcement of the Act, is essentially the same as the grand jury's, or the court's in issuing other pretrial orders for the discovery of evidence, and is governed by the same limitations." Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186, 216 (1945)).

124 United States v. First National Bank of Mobile, 295 F. 142 (S.D. Ala. 1924), *aff'd* 267 U.S. 576 (1924).

125 First National Bank of Mobile v. United States, 160 F.2d 532 (5th Cir. 1947); Falsone v. United States, 205 F.2d 734 (5th Cir. 1953) (requiring public certified accountant to produce taxpayers' books and records, even though the relationship between taxpayers and accountant was considered confidential); In re Albert Lindley Lee Memorial Hospital, 209 F.2d 122 (2d Cir. 1953) (names and addresses of patients confined in 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 (2d Cir. 1959); Bouschor v. United States, 316 F.2d 451 (8th Cir. 1963); United States v. Continental Bank & Trust Company, 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. Q. 277 (Jun. 1958, No.3); A. Sherwood Godwin, Jr., Note, *Constitutional Law—Attorney's Rights under Fifth Amendment to Withhold Client's Tax Records from Internal Revenue Service*, 9 WAKE FOREST L. REV. 561 (Dec. 1973, No.4); Lynn Katherine Thompson, Note, *IRS Access to Bank Records; Proposed Modifications in Administrative Subpoena Procedure*, 28 HASTINGS L.J. 247 (Sep. 1976, No.1).

126 Securities Act of 1933 § 8(e), Pub. L. 73–22, 48 Stat. 74 (1933), 15 U.S.C. §77a (for judicial interpretation of Section 8(e)); *see* McGarry v. Securities and Exchange Commission, 147 F.2d 389 (10th Cir. 1945); *see also* Donald R. C. Pongrace, Comment, *Requirement of Notice of Third-Party Subpoenas Issued in SEC Investigations: A New Limitation on the Administrative Subpoena Power*, 33 AM. U. L. REV. 701 (1984, No.3).

127 Oklahoma Press Publishing Co. v. Walling, 327 U.S. 186 (1945).

Communication Commission for inspections.[128] In *Newfield v. Ryan*,[129] a constitutional issue was raised calling into question the validity of subpoena *duces tecum*. Here, the SEC issued subpoena *duces tecum* to Western Union which required production of telegrams related to a Class A common stock. Petitioners challenged the constitutionality of the subpoenas. Judge Hutcheson, writing for a unanimous court, held that "the subpoenas do not take plaintiff's property, nor invade their right of privacy in the messages, inspection of which is demanded."[130] This is an early claim that telegraphic messages were the property of Western Union, not those of the business who sent the messages or received the messages. This position was later taken by the United States Supreme Court in *Smith v. Maryland* as the foundation for its third-party doctrine.[131]

B. Telephone, Wiretapping, and Section 605

In 1895, New York City began tapping telephones to collect evidence in criminal investigations.[132] As wiretapping became more widespread, the United States Supreme Court insisted on a narrower interpretation of the Fourth Amendment. It declared that wiretapping did not violate the Fourth Amendment in *Olmstead v. United States*.[133] In the courtroom, major telephone companies including AT&T, Pacific Telephone and Telegraph Company, United State Independent Telephone Association, and the Tri-State Telephone and Telegraph Company, submitted their briefs as *amici curiae* to support a broader notion of

---

128 Federal Communications Act of 1934, Pub. L. 73–416, 48 Stat. 1064 (Jun. 19, 1934); 47 U.S.C.A. §605; MAX D. PAGLIN, A LEGISLATIVE HISTORY OF THE COMMUNICATIONS ACT OF 1934 (1989) (Section 220(c) of the Act provides:

> The Commission shall at all times have access to and the right of inspection and examination of all accounts, records, and memoranda, including all documents, papers, and correspondence now or hereafter existing, and kept or required to be kept by such carriers, and the provisions of this section respecting the preservation and destruction of books, papers, and documents shall apply thereto. The burden of proof to justify every accounting entry questioned by the Commission shall be on the person making, authorizing, or requiring such entry and the Commission may suspend a charge or credit pending submission of proof by such person. Any provision of law prohibiting the disclosure of the contents of messages or communications shall not be deemed to prohibit the disclosure of any matter in accordance with the provisions of this section.

129 Newfield v. Ryan, 91 F.2d 700 (5th Cir. 1937).

130 *Id.* at 703.

131 Smith v. Maryland, 442 U.S. 735 (1979). For discussion, *see infra* Part III, Section C.

132 BRIAN HOCHMAN, THE LISTENERS: A HISTORY OF WIRETAPPING IN THE UNITED STATES 59 (2022).

133 Olmstead v. United States, 277 U.S. 438, 450 (1928).

unreasonable search.[134] These telephone companies tied their claim of privacy with property: "A third person who taps the lines violates the property rights of both persons then using the telephone, and of the telephone company as well."[135] The telephone companies also addressed the issue of contemporary American life: "The telephone has become part and parcel of the social and business intercourse of the people of the United States, and the telephone system offers a means of espionage compared to which general warrants and writs of assistance were the puniest instruments of tyranny and oppression."[136] Neither point found a sympathetic ear in the Supreme Court in 1928.

During the 1930s, records of calls by telephone companies began to be used as evidence and courts found them admissible without much difficulty.[137] In 1941, the Second Circuit held in *United States v. Gallo* that "[w]hen a person takes up a telephone he knows that the company will make, or may make, some kind of a record of the event, and he must be deemed to consent to whatever record the business convenience of the company requires."[138]

In the 1950s, the pen register, a device that could record the numbers dialed on telephones, came into the market.[139] Given the growing concerns regarding privacy in American society at this time,[140] evidence generated by pen register was

---

134 *Id*. at 452.

135 *Id*. 453.

136 *Id*. 454.

137 Blakeslee v. United States, 32 F.2d 15, 18 (1st Cir. 1929) ("We think it was competent, even if a remote fact, to show means of long-distance communication among the alleged conspirators. For this purpose, the strict identity of persons speaking over the phone was not necessary."); United States v. Radov, 44 F.2d 155 (3d Cir. 1930); United States v. Easterday, 57 F.2d 165, 167 (2d Cir. 1932) (noting in the opinion that telephone slips were put in evidence, but appellants "did not raise any question as to the competency of the papers." Therefore, "the objection is not now available."); Brink v. United States, 60 F.2d 231, 234 (6th Cir. 1932) ("There is no merit in these assignments [of error]. These telephone records tend to corroborate the testimony of the government's witnesses Faehr and Marshall. They were competent and their weight was a question for the jury."); Wood v. United States, 84 F.2d 749, 751 (5th Cir. 1936) (responding to appellant Wood's argument for inadmissibility of records of telephone calls, "They were introduced for the purpose of showing constant communication between Wood and his coconspirators, and were merely corroborative of other testimony.").

138 United States v. Gallo, 123 F.2d 229, 231 (2d Cir. 1941).

139 An early case challenging the use of pen register was Schmukler v. Ohio-Bell Tel. Co., 116 N.E.2d 819 (Ohio Ct. Com. Pl. 1953) (ruling that telephone company's use of pen register to monitor its services did not violate user's privacy) (In the 1960s, pen register was increasingly used in criminal investigations, as a result, cases questioning admissibility of pen register data as evidence flooded state and federal courts).

140 SAMUEL DASH, RICHARD F. SCHWARTZ & ROBERT E. KNOWLTON, THE EAVESDROPPERS (1959); *The Wiretapping-Eavesdropping Problem: Reflections on The Eavesdroppers: A Symposium*, 44 MINN. L. REV. 808 (1959-1960, No.5) (during the 1950s and 1960s, an increasing body of literature on privacy emerged in law reviews); *see* Alan F. Westin, *The Wire-Tapping Problem: An Analysis and a Legislative Proposal*, 52 COLUM. L. REV. 165 (Feb. 1952, No.2); Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I—The Current Impact of Surveillance on Privacy*, 66 COLUM.

frequently challenged in federal courts and often found inadmissible under Section 605 of the Federal Communications Act.[141] In *United States v. Guglielmo*, a federal district court stated that "unconsented use of a pen register violated the integrity of the telephone communications and the clear prohibition of §605."[142] Another federal district court in *United States v. Caplan* found the use of pen register constituted "interception," and therefore was not permissible.[143] The court recognized that ". . . Congress has indicated a policy of protecting the privacy of telephone subscribers from invasion by law enforcement officers . . . ."[144] The Seventh Circuit endorsed the ruling in *Guglielmo* and agreed with *Caplan* that the use of pen register constituted interception.[145] The Seventh Circuit stated that "we cannot pretend that the Government, while not hearing any verbal communication, did not inferentially have a reasonably good notion of the general substantive nature of the communications the pen register indicated where being initiated."[146] Furthermore, "[i]n circumstances such as those in this case, knowledge of the existence of the communication is knowledge of its likely character."[147]

After the Supreme Court decisions in *Katz v. United States* and *Berger v. New York*,[148] the United States Congress passed the Omnibus Crime Control and

---

L. REV. 1003 (Jun. 1966, No.6); Alan F. Westin, Part II, 66 COLUM. L. REV. 1205 (Nov. 1966, No.7); Donald B. King, *Electronic Surveillance and Constitutional Rights: Some Recent Developments and Observations*, 33 GEO. WASH. L. REV. 240 (Oct. 1964, No.1); Donald B. King & Marwin A. Batt, *Wire Tapping and Electronic Surveillance: A Neglected Constitutional Consideration*, 66 DICK. L. REV. 17 (1961, No.1); Charles B. Nutting, *Public Policy and the Problem of Electronic Surveillance*, 48 A.B.A. J. 676 (Jul. 1962, No.7); W. H. Parker, *Surveillance by Wiretap or Dictograph: Threat or Protection: A Police Chief's Opinion*, 42 CALIF. L. REV. 727 (Dec. 1954, No.5).

141 Federal Communications Act of 1934 § 605, Pub. L. 73-416, 48 Stat. 1064 (Jun. 19, 1934) ("No person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee . . . ."));Victor S. Elgort, Note, *Legal Constraints Upon the Use of the Pen Register as a Law Enforcement Tool*, 60 CORNELL L. REV. 1028 (Aug. 1975, No.6); United States v. Guglielmo, 245 F.Supp. 534, 535 (N.D. Ill. 1965); United States v. Caplan, 255 F.Supp. 805, 807 (E.D. Michi. 1966); Floyd E. Siefferman, Jr., Note, *"Interception" in Telephonic Communications under Section 605 of the Federal Communications Act*, 8 J. PUB. L. 318 (Spring 1959, No.1).

142 United States v. Guglielmo, 245 F.Supp. 534, 536 (N.D. Ill. 1965), *aff'd* United States v. Dote, 371 F.2d 176 (7th Cir. 1966).

143 United States v. Caplan, 255 F.Supp. 805, 808 (E.D. Mich. 1966).

144 *Id.* at 808.

145 United States v. Dote, 371 F.2d 176, 181 (7th Cir. 1966) ("The ringing of the telephone, therefore, may of itself be a communication, and a device, attached to the telephone line, which indicates to a third party that such a communication is taking place or is about to take place, intercepts it.").

146 *Id.*

147 *Id.*

148 Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967).

Safe Streets Act of 1968.[149] Driven by concerns about "organized crime,"[150] the 1968 Act amended Section 605 by inserting "except as authorized by chapter 119, title 18, United States Code."[151] Chapter 119 explicitly allowed interceptions by employees of communication common carrier, agents of FTC, undercover agents party to the communication, and persons under color of law who had been given prior consent by one of the parties to the communication.[152] It also authorized the President to act when national security was concerned.[153] These exceptions soon eroded Section 605 as a solidary norm on privacy.

A marked increase in subpoenas directed at telephone companies was accompanied with various circuit court cases.[154] In *United States v. Covello*,[155] the Second Circuit distinguished pen registers from the toll records of a telephone company: "The keeping of toll records is a necessary part of the ordinary course of the telephone company's business and is necessary in order that the company may substantiate its charges to its customers."[156] Therefore, the court claimed, "Section 605 was not designed to render evidentially inadmissible the records made in the ordinary course of the telephone company's business and which are essential to the ordinary operation of that business."[157] This ruling was followed by the Sixth Circuit,[158] and the Seventh Circuit.[159]

The Second Circuit soon had another chance to look into the issue in 1976,[160] which eventually led to a significant decision by the Supreme Court of the United States in *United States v. New York Telephone Co*.[161] The major question

---

149 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 197 (June 19, 1968), codified at 34 U.S.C. § 10101 et seq.); *see* JAMES G. CARR, *The Enactment and Consitutionality of Title III*, THE LAW OF ELECTRONIC SURVEILLANCE 21-62 (1977) (providing a legislative history).

150 S. Rep. No.1097, 90th Cong., 2d Sess. 40 (1968), reproduced 1968 U.S.C.C.A.N. 2112 (stating "[t]he major purpose of title III is to combat organized crime."; *see also Controlling Crime Through More Effective Law Enforcement: Hearings Before the United States Senate Committee on the Judiciary*, 90th Cong., 1st Sess. (Mar. 7-9, Apr. 18-20, May 9, July 10-12, 1967); CHALLENGE OF CRIME IN A FREE SOCIETY: A REPORT BY THE PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE (1967).

151 Section 803, 82 Stat. at 223.

152 *Id*.

153 United States v. Caplan, 255 F.Supp. 805, 808 (E.D. Michi. 1966).

154 James E. Burke, Comment, *Judicial Coercion of Unwilling Telephone Companies in Pen Register Cases*, 45 U. CIN. L. REV. 649 (1976, No.4); Note, *Circumventing Title III: The Use of Pen Register Surveillance in Law Enforcement*, 1977 DUKE L.J. 751 (Aug. 1977, No.3).

155 United States v. Covello, 410 F.2d 536 (1969).

156 *Id*. at 542.

157 *Id*.

158 DiPiazza v. United States, 415 F.2d 99 (6th Cir. 1969).

159 United States v. Finn, 502 F.2d 938 (7th Cir. 1974).

160 In re Application of the United States in the Matter of an Order Authorizing the Use of a Pen Register or Similar Mechanical Device, 538 F.2d 956 (1976), *rev'd sub nom.* United States v. New York Tel. Co., 434 U.S. 159 (1977).

161 United States v. New York Tel. Co., 434 U.S. 159 (1977).

of this case was whether a federal district court could 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. To install the pen register in an unobtrusive fashion, the FBI needed an unused telephone line (known as "leased line") connected with the subject telephone line. The telephone company refused.[162] The Court was emphatic on the difference between log information and contents, insisting that "[p]en registers do not 'intercept' because they do not acquire the 'contents' of communications."[163] To be more specific, "[t]hese devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication."[164] Based on this crucial difference, the Court concluded that "Congress did not view pen registers as posing a threat to privacy of the same dimension as the interception of oral communications and did not intend to impose Title III restrictions upon their use."[165]

Two years later, in *Smith v. Maryland*,[166] the Supreme Court ruled that a. pen register was not a "search," and therefore, not a violation of the Fourth Amendment. The *Smith* Court suggested two prongs:[167] first, whether the individual has exhibited an actual or subjective expectation of privacy; and second, whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable. In *Smith*, the pen register was installed on telephone company property in the latter's central offices.[168] Regarding this issue, the Court stated, "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[169] It also said that: "petitioner voluntarily conveyed to [telephone company] information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police."[170]

In sum, the judiciary was not keen on the Fourth Amendment before the internet arrived.[171] This was largely based on the legacy inherited from the telegraph era and interests in the data gathering function of private sectors—banks,

---

162 *Id*. at 162.

163 *Id*. at 167.

164 *Id*. at 167.

165 *Id*. at 168.

166 Smith v. Maryland, 442 U.S. 735 (1979).

167 *Id*. at 740.

168 *Id.* at 741.

169 *Id*. at 743-44.

170 *Id*. at 745; *see* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (Aug. 2004, No.6) (The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy and the USA Patriot Act).,

171 Silas J. Wasserstrom, *The Incredible Shrinking Fourth Amendment*, 21 AM. CRIM. L. REV. 257, 259 (Winter 1984, No.3) ("Over the past ten years, as its composition has changed, the [United States Supreme] Court has become both increasingly hostile toward the exclusionary rule and increasingly indulgent toward the police.").

accountants, employers, and even newspapers.[172] A federal court took notice of the fact that between January 1971 and March 1974, AT&T received 75,000 to 100,000 toll-record subpoenas, which translated to 2,000 to 3,000 subpoenas each month.[173] AT&T, like Western Union, resisted the pressure by adopting the notification policy in March 1974,[174] to no avail.

C. The Stored Communication Act

The Stored Communication Act (SCA),[175] was enacted in 1986 as Title II of the Electronic Communications Privacy Act of 1986 (ECPA).[176] The powers of government were further strengthened when Congress passed the Communications Assistance for Law Enforcement Act (CALEA) of 1994,[177] and the USA Patriot Act of 2001.[178]

The 1986 ECPA reflected the grand bargaining in the 1980s between the Department of Justice on the one hand and the telecom industry and privacy groups on the other.[179] It was around this time that AT&T was broken up, and new

---

172 Donaldson v. United States, 400 U.S. 517 (1971) (superseded by statute, 26 U.S.C.A. § 7609, as recognized in Tiffany Fine Arts, Inc. v. United States, 469 U.S. 310 (1985)); United States v. Miller, 425 U.S. 435 (1976); Zurcher v. Stanford Daily, 436 U.S. 547 (1978). Shirley M. Hufstedler, *Invisible Searches for Intangible Things: Regulation of Governmental Information Gathering*, 127 U. PA. L. REV. 1483, 1503-07 (Jun. 1979, No.6); Branzburg v. Hayes, 408 U.S. 665 (1972); Donna M. Murasky, *Journalist's Privilege:* Branzburg *and Its Aftermath*, 52 TEX. L. REV. 829 (May 1974, No.5); James S. Liebman, Note, *Search and Seizure of the Media: A Statutory, Fourth Amendment and First Amendment Analysis*, 28 STAN. L. REV. 957 (May 1976, No.5); Monica Langley & Lee Levine, Branzburg *Revisited: Confidential Sources and First Amendment Values*, 57 GEO. WASH. L. REV. 13 (Nov. 1988, No.1); *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735 (1984).

173 Reporters Committee for Freedom of Press v. AT&T, 593 F.2d 1030, 1039 (D.C. Cir. 1978).

174 *Id*. at 1038.

175 Stored Communication Act ("SCA"), 18 U.S.C. §2701 et seq.

176 Electronic Communications Privacy Act of 1986, PL 99-508, Oct. 21, 1986, 100 Stat. 1848 ("ECPA").

177 Communications Assistance for Law Enforcement Act ("CALEA") of 1994, Pub. L. No. 103-414, Oct. 25, 1994, 108 Stat. 4279, codified at 47 U.S.C. §§1001-10 (2020); *see*, Susan Freiwald, *Uncertain Privacy: Communication Attributes after the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (Mar. 1996, No.3).

178 USA Patriot Act of 2001, *supra* note 15.

179 *See* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 109-43 (1995) (on the legislative process of ECPA) [hereinafter REGAN, LEGISLATING PRIVACY]; Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (Aug. 2004) (the Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy and the USA Patriot Act) [hereinafter Kerr, *A User's Guide*]; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (Aug. 2004) [hereinafter Mulligan, *Reasonable Expectations*].

technologies such as cellular phone services and computer networks (e.g., email) became significant. SCA created a framework for law enforcement to have access to contents of communication and subscriber data by different legal instruments.[180] Access to contents of communication that had been recorded within the past 180 days had the most strict and simple rule: a warrant.[181] Access to contents of communication that had been recorded more than 180 days prior depended on whether notice was given to the subscriber. Those situations included: (1) obtaining a warrant if access was discrete, i.e., no notice to the subscriber;[182] (2) an administrative subpoena, or grand jury subpoena, or a court order was required if access was open, i.e., prior notice to the subscriber.[183] For access to non-content data, either a warrant, administrative subpoena, grand jury subpoena, or court order would be adequate.[184]

In 1986, Senator Patrick J. Leahy considered allowing law enforcement access to the electronic communication systems with the condition of court order to be a good balance of security and privacy.[185] That balance, however, was questioned by the Justice Department and renegotiated during the Bush and Clinton administrations,[186] which resulted in CALEA in 1994. CALEA requires telecommunication carriers and equipment manufacturers to build into their networks technical capabilities to assist law enforcement with authorized interception of communications and call-identifying information.[187] Furthermore, CALEA amended Section 2703 by adding a subsection that allowed law enforcement to access subscriber information by an administrative subpoena or grand jury subpoena.[188] This was a clarification from the earlier text of Section 2703 and enabled law enforcement's ready access to the "big data" in the eve of the coming internet. After the September 11 attacks, this same subsection in Section

---

180 Electronic Communications Privacy Act tit. II, § 2703.

181 *Id.* § 2703(a).

182 *Id.* § 2703(b)(A).

183 *Id.* § 2703(b)(B).

184 *Id.* § 2703(c)(B).

185 *Prepared Statement of Senator Patrick J. Leahy*, *in* Hearing before the Subcommittee on Patents, Copyrights and Trademarks of the Committee on the Judiciary, United States Senate Ninety-ninth Congress First Session on S. 1667 (Nov. 13, 1985) (Serial No. J-99-72), at 43. S. Rep. No. 99-541 (Oct. 17, 1986).

186 *Statement of Louis J. Freeh, Director, Federal Bureau of Investigation*, in DIGITAL TELEPHONY AND LAW ENFORCEMENT ACCESS TO ADVANCED TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES (Joint Hearings before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary), Mar. 18, 1994 [hereinafter DIGITAL TELEPHONY].

187 Communications Assistance for Law Enforcement Act § 103, codified as 47 U.S.C. § 1002; *United States Telecom Association v. FCC*, 227 F.3d 450 (D.C. Cir. 2000) (telecommunication carriers and privacy groups challenging an order by FCC requiring carriers to ensure that their systems were technically capable of enabling law enforcement agencies intercepting telephone calls and obtaining certain call-identifying information).

188 Communications Assistance for Law Enforcement Act § 207.

2703 that allowed subscriber information to be obtained by administrative subpoena or grand jury subpoena was further expanded by the USA Patriot Act in 2001.[189]

In sum, from its creation in 1986, SCA was expanded by CALEA and then the USA Patriot Act, which primarily increased the power of the law enforcement to access data via administrative subpoena and grand jury subpoena. In that sense, SCA embodies the core of the symbiotic relationship between the telecommunication industry and the surveillance state, with the latter clearly driving the bargaining process.[190]

D. Comparative Perspective

State ownership was closely related to the interaction between the State and the telecom sector. In 1957, the British Parliament initiated an inquiry into the "state of law" on telephone interceptions, which resulted in the Birkett Report.[191] The Report noted that while its legal foundation was "obscure,"[192] it was a practice "since the introduction of the telephone."[193] Prior to 1937, the interception of telephone communication was arranged between police authorities and the Director-General of the Post Office.[194] In 1937, the Home Secretary and the Postmaster-General decided that the Post Office could only intercept telephone conversations by express warrant of the Secretary of State.[195] This "obscurity" remained unchanged until it got more attention in 1979, when the first wiretapping case was brought to English Court in *Malone v. Metropolitan Police Commissioner*.[196] James Malone, an antique dealer, was charged with offences relating to stolen property. During trial, the prosecution admitted that there was an interception of Malone's phone line. Malone filed an interlocutory motion on the issue that tapping was unlawful. Here, tapping was conducted by Post Office officials who then made the recordings available to police for the purposes of

---

189 USA Patriot Act § 210, codified as 18 U.S.C. §2703(c)(2); (USA FREEDOM Act), 129 Stat. 268 (2015) (in June 2015, Congress passed Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act amending the Foreign Intelligence Surveillance Act of 1978 but not the SCA discussed in this article).

190 *See* DIGITAL TELEPHONY, *supra* note 186 (The dialogue between Senator Leahy and FBI Director Louis J. Freeh during the 1994 congressional hearing is perhaps the best demonstration of this. Senator Leahy, the main architect of ECPA of 1986, kept asking Freeh, "[w]hat I am concerned about is, why is current law inadequate?").

191 REPORT OF THE COMMITTEE OF PRIVY COUNCILORS APPOINTED TO INQUIRE INTO THE INTERCEPTION OF COMMUNICATIONS: PRESENTED TO PARLIAMENT BY THE PRIME MINISTER BY COMMAND OF HER MAJESTY (Cmnd 283) (Oct. 1957) (Birkett Report).

192 *Id.* para. 9.

193 *Id.* para. 40.

194 *Id.* para. 40.

195 *Id.* para. 41.

196 *Malone v. Metropolitan Police Commissioner (No.2)*, [1979] EWHC 2 (Ch), [1979] Ch. 344, [1979] 2 All E.R. 620; *see also* WALTER H. ZEYDEL, WIRE TAPPING AS EVIDENCE IN COURT IN GREAT BRITAIN AND THE BRITISH COMMONWEALTH OF NATIONS (Library of Congress American-British Law Division 1961) (mimeograph).

transcription and use.[197] The presiding judge, Vice-Chancellor Sir Robert Megarry, found that Malone's claim failed in its entirety.[198] The judge ruled that the Post Office did not trespass by tapping Malone's phone line because "all that is done is done within the Post Office's own domain."[199] Tapping was not an offence because it was information "obtained by a Crown servant in the course of his duty or under the authority of the Postmaster General . . ."[200]

Malone's case was brought to the European Court of Human Rights, and in August 1984, the European Court ruled against the United Kingdom.[201] The European Court found interception of communications constituted an interference with Malone's Article 8 rights—respect for private life and correspondence—and it was not "in accordance with the law."[202] Even before the European Court's decision was officially publicized, in April 1984, the British government under Margaret Thatcher privatized British Telecom (BT).[203] Furthermore, in order to comply with the European Court's ruling, the Thatcher government rushed to introduce a bill that became the Interception of Communications Act 1985.[204] For the first time, Britain brought wiretapping under an open legal framework.

Britain led the privatization of the telecommunication industry across Europe.[205] The Dutch PTT (Post, Telegraph and Telephone Company) was reformed in 1989, and the telecommunication market in the Netherlands was gradually liberalized between 1991 and 1997.[206] In Germany, the state-owned Deutsche Telekom AG was transformed to partially private corporation in January

---

197 *Malone*, [1979] Ch. 344 at 355.

198 *Id*. at 383.

199 *Id*. at 369.

200 *Id*. at 378.

201 *Malone v. the United Kingdom*, Judgment (Merits), App No 8691/79 (A/82), [1984] ECHR 10, (1984) 7 Eur. H. R. Rep. 14, IHRL 47 (ECHR 1984), European Court of Human Rights (August 2, 1984).

202 *Id*. para. 80.

203 *See* Mark Thatcher, *Liberalization in Britain: From Monopoly to Regulation of Competition*, in EUROPEAN TELECOMMUNICATIONS LIBERALIZATION 93-109 (Kjell A. Eliassen & Marit Sjøvaag eds. 1999) (in 1984, the British government sold 51 per cent of BT's shares to private investors; the remaining public stake was sold in 1990 and 1993); WILLEM HULSINK, PRIVATIZATION AND LIBERALIZATION IN EUROPEAN TELECOMMUNICATIONS: COMPARING BRITAIN, THE NETHERLANDS AND FRANCE 111-69 (1999) (Chapter 4. The Liberalization, Privatization and Regulatory Reform of Telecommunications in the UK: In Case of the Market?).

204 Interception of Communications Act, 1985 c. 56. For the legislative process and substance of the 1985 Act, *see* Ian J. Lloyd, *The Interception of Communications Act 1985*, 49 MOD. L. REV. 86 (Jan. 1986, No.1); Ian Cameron, *Telephone Tapping and the Interception of Communications Act 1985*, 37 NORTH. IRE. LEGAL Q. 126 (Summer 1986, No.2).

205 *See generally* JOHAN FROM, THE PRIVATIZATION OF EUROPEAN TELECOMMUNICATIONS (2017); EUROPEAN TELECOMMUNICATIONS LIBERALIZATION (Kjell A. Eliassen & Marit Sjovaag eds. 1999); WILLEM HULSINK, *supra* note 203.

206 WILLEM HULSINK, *supra* note 203, pp.170-224 (Chapter 5. The Liberalization, Privatization and Regulatory Reform of Telecommunications in the Netherlands).

1995.[207] France Télécom was corporatized by the end of December 1996 and partially privatized in October 1997.[208]

The increasing concerns of privacy in Europe during the 1960s led to legislative efforts in the 1970s characterized by comprehensive data legislations.[209] Writing in 1989, David H. Flaherty observed that "European data protection laws include the hidden agenda of discouraging a recurrence of the Nazi and Gestapo efforts to control the population,"[210] and "[t]his concern is such a vital foundation of current legislation that it is rarely expressed in formal discussions."[211] However, Flaherty also noted the difficulties that the data protection commissions within bureaucratic structures. Flaherty noted that it was "[g]overnment agencies [that] are the leading invaders of the personal privacy of citizens,"[212] since they maintain systems with the largest scope and most numerous records. Therefore, Flaherty concluded that "[t]he ultimate protection for the individuals is the constitutional entrenchment of rights to privacy and data protection."[213]

The *Malone* case and the long history of wiretapping in Great Britain suggest that the domestic processes—legislative and judicial—failed to deliver constitutional protection of privacy. It was the European Court of Human Rights—a supernational judiciary—that provided the crucial function of constitutional adjudication. Similarly, in *Klass v. Germany*,[214] the European Court pointed to the

---

207 Peter Kespohl, *25 Years of Deutsche Telekom AG – From State-owned Enterprise to Stock Corporation*, Jan. 2, 2020, https://www.telekom.com/en/media/media-information/archive/25-years-of-deutsche-telekom-ag-589922 (last access Oct. 10, 2022); *see* Raymund Werle, Liberalization of Telecommunications in Germany, in EUROPEAN TELECOMMUNICATIONS LIBERALIZATION 110-27 (Kjell A. Eliassen & Marit Sjøvaag eds. 1999) (on the privatization of the telecom sector in Germany).

208 HULSINK, *supra* note 203, at 225-78

209 DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES: THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA AND THE UNITED STATES (1989); FRITS W. HONDIUS, EMERGING DATA PROTECTION IN EUROPE (1975); Frits W. Hondius, *Data Law in Europe*, 16 STAN. J. INT'L L. 87 (1980); Paul M. Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675 (Fall 1989, No.4); Helen Trouille, *Private Life and Public Image: Privacy Legislation in France*, 49 INT'L & COMP. L.Q. 199 (Jan. 2000, No.1).

210 FLAHERTY, at 373.

211 *Id*, at 374.

212 *Id*, at 375.

213 *Id*. at 376.

214 Klass v. Federal Republic of Germany, Judgment, Merits, App no 5029/71 (A/28), (1979-80) 2 Eur. H. R. Rep. 214, IHRL 19 (ECHR 1978), 6th September 1978, European Court of Human Rights [ECHR]; Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 Hastings L.J. 751 (2002-2003) (hereinafter, Paul M. Schwartz, *Law Enforcement Surveillance*); Paul M. Schwartz, *Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Planck Institute's Study*, 72 GEO. WASH. L. REV. 1244 (Aug. 2004, No.6) (The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & (and) the USA Patriot Act: Surveillance Law: Reshaping the Framework); James G. Carr, *Wiretapping in West Germany*, 29 AM. J. COMP. L. 607 (Fall 1981, No.4).

direction of reform in Germany's wiretapping law. In France, the European Court's ruling in *Kruslin v. France* and *Huvig v. France*,[215] helped push the French Parliament to pass the 1991 Wiretapping Act.[216] The supernational adjudication by the European Court became a powerful voice of privacy as a constitutional value during the early 1990s.

By contrast, democracies without the benefit of such a supernational judiciary relied on domestic social and political dynamics. Canada, for example, embraced constitutional recognition of privacy in 1982 by Section 8 of the Canadian Charter of Rights and Freedoms.[217] In 1985, Canada amended its Criminal Code to bring wiretapping under judicial control.[218] Japan is another example. The Constitution of Japan provides protection of privacy in Article 35, which transplants the Fourth Amendment to Japan.[219] In post-World War II Japan, like in Europe, the

---

215 Kruslin v. France, Judgment (Merits), App No 11801/85, [1990] ECHR 10, (1990) 12 Eur. H. R. Rep. 547 (April 24, 1990). Huvig v. France, Judgment (Merits), App No 11105/84, A/176-B, (1990) 1 Eur. H. R. Rep. 528, IHRL 96 (ECHR 1990), 24th April 1990 [ECHR].

216 Wiretapping Act, Loi nº 91-646 of July 10, 1991; *see*, generally, Edward A. Tomlinson, *The Saga of Wiretapping in France: What It Tells Us about the French Criminal Justice System*, 53 LA. L. REV. 1091 (Mar. 1993, No.4).

217 Constitution Act 1982, Schedule B to the Canada Act 1982, 1982, c. 11 (U.K.) (section 8 of the Canadian Charter of Rights and Freedoms provides: "Everyone has the right to be secure against unreasonable search or seizure.");,
Hunter v. Southam, Inc., [1984] 2 R.C.S. 145, (adopting Katz's statement that "the Fourth Amendment protects people, not places" in interpreting s. 8 of the Charter); *R. v. Grant*, [1993] 3 R.C.S. 223 (Sup. Ct. Canada) (holding that police violated s. 8 of the Charter for conducting perimeter search without a warrant); R. v. Wiley, [1993] 3 R.C.S. 263 (Sup. Ct. Canada) (holding that the warrantless perimeter search of the accused's residence was unreasonable and therefore in violation of s. 8 of the Charter); R. v. Plant, [1993] 3 RCS 281 (Sup. Ct. Canada) (holding that the perimeter search without warrant was unreasonable and violated s. 8 of the Charter); James Stribopoulos, *In Search of Dialogue: The Supreme Court, Police Powers and the Charter*, 31 QUEEN'S L.J. 1 (Fall 2005, No.1); Jane Bailey & Sara Shayan, *Systematic Government Access to Private-Sector Data in Canada*, in BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 147-72 (Fred H. Cate & James X Dempsey eds. 2017).

218 Section 487.014(1) of the Criminal Code, R.S.C. 1985, c. C-46.

219 Nippon Koku Kenpo 日本国憲法 [The Constitution of Japan] (2017); *The Constitution of Japan*, 53 L. & CONTEMP. PROBS. 201, 205 (1990) Article 35 provides,

> "The right of all persons to be secure in their homes, papers and effects against entries, searches and seizures shall not be impaired except upon warrant issued for adequate cause and particularly describing the place to be searched and things to be seized, or except as provided by Article 33."
> Each search or seizure shall be made upon separate warrant issued by a competent judicial officer.

general public was very sensitive to governmental intrusion of privacy.[220] Even though Japan did not suffer from terrorist attacks, similar to the September 11th incident, or the London bombing, there was still an abundance of concern. In March 1995, the Tokyo subway poisonous gas attacks, known as the Tokyo Sarin Attacks (地下鉄サリン事件) occurred.[221] Concerns about organized crime was one key driving force behind the 1999 Communications Interception Act,[222] the first law in Japan, which formally allowed wiretapping by law enforcement. The Act went through enormous controversy, with strong opposition from employees of the telecommunication industry, internet service providers, academics, and the bar.[223]

---

220 Motohiro Tsuchiya [土屋大洋], *Systematic Government Access to Private-Sector Data in Japan*, *in* BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 275–85 (Fred H. Cate & James X. Dempsey eds., 2017).

221 Masaki Kawasumi [川澄真樹], 組織犯罪・テロに対する刑事訴追目的での通信傍受 [*Wiretapping in Response to Prosecution of Organized Crimes and Terror*], 45 *Daigakuin Kenkyu Nenpō* [大学院研究年報] (ANNUAL OF GRADUATE SCHOOL) 315, 316 (Feb. 2016). Curtis J. Milhaupt & Mark D. West, *The Dark Side of Private Ordering: An Institutional and Empirical Analysis of Organized Crime*, 67 U. CHI. L. REV. 41 (2000); Mark D. West, *Information, Institutions, and Extortion in Japan and the United States: Making Sense of Sokaiya Racketeers*, 93 NW. U. L. REV. 767 (1999).

222 Hanzai sosa no tame no tsushin bōju ni kansuru hōritsu 犯罪捜査のための通信傍受に関する法律 [Communications Interception Act] (Law No. 137) Aug. 18, 1999. For an English translation of the 1999 Act, Yohei Suda, *Translation, The Japanese Law on Communications Interception During Criminal Investigations*, 10 PAC. RIM L & POL'Y J. 67 (2000). For commentaries, Lillian Roe Gilmer, Note, *Japan's Communications Interception Act: Unconstitutional Invasion of Privacy or Necessary Tool*, 35 VAND. J. TRANSNAT'L L. 893 (2002).

223 Lillian Roe Gilmer, *supra* note 222, at 900–02. One strong opponent was Kazushi Teranishi (寺西和史), an Assistant Judge at Sendai District Court at the time. Judge Teranishi wrote and spoke against the legislation and was disciplined for engaging in political activities. The case went all the way to the Supreme Court of Japan, which upheld the disciplinary penalty. *See*, 最高裁判所大法廷 [Grand Chamber of the Supreme Court of Japan], 民集第 52 巻 9 号 1761 頁 [52 Minshu 1761, Dec. 1, 1998; *see* Daniel H. Foote, *Restrictions on Political Activity by Judges in Japan and the United States: The Cases of Judge Teranishi and Justice Sanders*, 8 WASH. U. GLOBAL STUD. L. REV. 285 (2009) (Law in Japan: A Celebration of the Works of John Owen Haley). Scholars voiced their concerns for citizens' constitutional liberty; *Horitsu Jihō* 法律時報 [*Law Times*] devoted a special October 1999 issue to the debate on the Act with the title "Wiretapping and Citizens' Liberty" (盗聴法と市民的自由), https://www.nippyo.co.jp/shop/magazine/4316.html (last accessed Jan. 13, 2022).

In December 1999, a few months after the 1999 Act was passed but before the Act took effect, the Supreme Court of Japan was presented a case on wiretapping, 最高裁判所第三小法廷 [The Third Petty Chamber of the Supreme Court of Japan], 刑集第 53 巻 9 号 1327 頁 [53 Keishu 1327 (No.9), Dec. 16, 1999](In this case, Hokkaidō prefecture's Asahikawa city police in an organized crime case applied for and obtained a search warrant to wiretap the telephone lines of suspects. Defendants questioned the constitutionality of the search. They contended that because the search infringed upon due process under Article 31 and privacy rights under Article 35 of Japan's Constitution, the police had to prove that there was no other means for their investigation other than wiretapping. The Supreme Court, however,

But Japan's experience was not fundamentally different from that of Europe. In July 1999, Nippon Telegraph and Telephone Company (NTT)—postwar Japan's powerful state-owned telephone company—finally concluded its privatization process which it had started in 1985. NTT was split into three.[224] One of the spin-offs, the NTT DoCoMo (NTT ドコモ) was to launch the world's first large-scale mobile internet service. The industry became private and diverse with multiple players. Japan's relationship with the government, including law enforcement, was changing. Thus, the 1999 Act in Japan and similar statutes in Great Britain and continental Europe prepared the structure for a symbiotic relationship.

IV. INTERNET AND THE ENTRENCHED SYMBIOTIC MODEL

The social media website, Facebook, was founded in February 2004.[225] If the social media giant represents the beginning of Web 2.0—the arrival of "surveillance capitalism"—it coincided with another major historical moment in America: the anti-terror war in the wake of the September 11th incident. The change of atmosphere was dramatic.[226] Telecommunication and internet service providers found themselves "caught in the middle."[227] Albert Gidari Jr., a lawyer who represented tech firms, noted that the September 11 attacks changed the relationship between law enforcement and service providers: "[t]he government no longer is patient with service providers who delay, argue, review process, complain about it, or push back."[228] It created the perfect beginning for the symbiotic model of surveillance state. This Part will discuss three areas of law related to this symbiotic relationship: the Fourth Amendment jurisprudence in Section A, which sets the foundation and constitutional outer limits for the relationship between surveillance capitalism and surveillance state. Sections B and C cover the legal framework regulating the interaction between surveillance capitalism and the surveillance state under the Stored Communications Act (SCA). Section B will be

---

did not touch on the Constitution and simply ruled that the search followed procedures required by law and thus the appeal was dismissed).

224 Marie Anchordoguy, *Nippon Telegraph and Telephone Company (NTT) and the Building of a Telecommunications Industry in Japan*, 75 BUS. HIST. REV. 507, 531 (Autumn 2001, No.3).

225 SHANE M. GREENSTEIN, HOW THE INTERNET BECAME COMMERCIAL: INNOVATION, PRIVATIZATION, AND THE BIRTH OF A NEW NETWORK 186 (Princeton, 2015).

226 Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (Jun. 2002, No.6) (Symposium: Modern Studies in Privacy Law); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (Jul. 2002, No.5); DAVID LYON, SURVEILLANCE AFTER SEPTEMBER 11 (2003).

227 Albert Gidari, Jr., *Companies Caught in the Middle*, 41 U.S.F. L. REV. 535 (Spring 2007) (Keynote Address at Symposium: Companies Caught in the Middle).

228 *Id*. at 541; *see also* LYON, *supra* note 226; Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance after September 11*, 54 HASTINGS L.J. 971 (2002-2003) (Symposium: Enforcing Privacy Rights); William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance after the Terror*, 57 U. MIAMI L. REV. 1147 (Jul. 2003).

focused on disclosure rules that enable law enforcement to have access to the data collected by the digital platforms from their users; and Section C will be focused on non-disclosure orders under SCA, which protects the secrecy of such disclosures. The goal of this Part is to present the current state of law that regulates government access of data in the symbiotic relationship. Section D presents a comparative perspective by discussing the development of surveillance states in the Commonwealth countries, the European Union, and Japan.

A. Reasonable Expectation of Privacy

Unlike many European countries, there is no comprehensive or general statute on privacy at the federal level in the United States.[229] The highest authority in this area is the Fourth Amendment of the United States Constitution, which protects citizens from unreasonable search and seizure.[230] Throughout history, one important function of the Supreme Court has been to define the scope of the Fourth Amendment. As mentioned earlier, in *Katz*,[231] the Court ruled that wiretapping a public phone booth without a warrant violated the Fourth Amendment. After *Katz*, the most representative decisions are *Smith v. Maryland* and *United States v. Miller*,[232] which both rely on the third-party doctrine. The arrival of the Internet and social media poses questions about whether legal doctrines developed in the analogue age are still good for the digital era.[233] The Court touched on police use of GPS and search of a cell phone upon arrest[234] in *Carpenter v. United States*.[235]

---

229 Paul M. Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321 (Jul. 1992). On the state level, the situation is changing. On July 7, 2021, Colorado enacted the Comprehensive Data Privacy Act (SB 21-190) (CCDPA), making Colorado the third state with such a privacy law in the United States. Virginia was the second state to enact a Consumer Data Protection Act (VCDPA), on Mar. 2, 2021. Both CCDPA and VCDPA will go into effect on Jan. 1, 2023. The first state was California, with the Consumer Privacy Act of 2018 (CCPA) and the California Privacy Rights Act of 2020 (CPRA).

230 U.S. Const. amend. IV

231 Katz v. United States, 389 U.S. 347 (1967).

232 Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

233 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 (Feb. 2009); Erin Murphy, *The Case against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (Summer 2009) (Symposium: Security Breach Notification Six Years Later).

234 United States v. Jones, 565 U.S. 400 (2012); Riley v. California, 573 U.S. 373 (2014).

235 Carpenter v. United States, 138 S.Ct. 2206 (2018).

We will start the discussion with the *Carpenter* case and the issue of cell-site location information, then subscriber information and Internet protocol (IP) addresses, and lastly to the murkier area—stored emails.

1. Cell-site Location Information

Cell-site location information (CSLI) are records generated when cell phones are connected to radio antennas installed on the cellular towers of wireless service companies. Questions regarding government access to CSLI were at the center of *Carpenter v. United States*.[236] Here, in a robbery case, Detroit police sought disclosure of certain telecommunication records from wireless carriers, MetroPCS and Sprint, under SCA, 18 U.S.C. § 2703(d). Federal Magistrate Judges issued two court orders, which allowed the government access to 127 days and 88 days of CSLI data, respectively.[237] The data was used in court as evidence 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, which was affirmed by the Sixth Circuit.[238] The Sixth Circuit considered two factors fundamental: (1) CSLI was considered metadata rather than content;[239] and (2) CSLI was a business record that Carpenter shared with his wireless carrier.[240] Guided by *Smith* as "the binding precedent," the Sixth Circuit ruled that *Carpenter* had no reasonable expectation for CSLI data privacy.[241]

---

236 *Id.*

237 There is 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. 235 at 2212; while the Sixth Circuit opinion suggested 127 days and 88 days in United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016).

238 United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *rev'd*, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018).

239 *Id*. 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.").

240 *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.").

241 *Id*. at 888 (ruling that "for the same reasons that Smith had no expectation of privacy in the numerical information at issue there, the defendants have no such expectation in the locational information here. On this point, *Smith* is binding precedent."). 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) (ruling 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. *In the Matter of* the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 313 (3rd Cir. 2010); *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Cuerrero, 768 F.3d 351, 358 (5th Cir. 2014) (ruling that the government violated SCA because it obtained historical cell site location data without

The Supreme Court of the United States, 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."[242] The majority held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[243]

In reaching its conclusion, the *Carpenter* majority did not address the content and non-content distinction—nor did the dissenting opinions. Rather, both the majority and the dissenters focused on the third-party doctrine. While still recognizing third-party doctrine as a general rule, the majority's main focus was to explain that CSLI data is a "qualitatively different category" of business records.[244] 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;"[245] that CSLI data "present[s] even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*."[246] Throughout the opinion, the majority emphasized the contrast between CSLI and traditional tools that police had:

> 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.[247]

This way, the majority was able to keep the third-party doctrine as a general rule,[248] but declared that Carpenter had reasonable expectation of privacy over his CSLI data.

---

a Section 2703(d) order; however, there was no violation of the Fourth Amendment); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (*en banc*); United States v. Graham, 824 F.3d 421, 428 (4th Cir. 2016) (*en banc*); United States v. Thompson, 866 F.3d 1149, 1160 (10th Cir. 2017).

242 Carpenter, 138 S.Ct. at 2217.

243 *Id*.

244 *Id.* at 2216–17 ("while 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.").

245 *Id*. at 2218.

246 *Id*.

247 Carpenter, 138 S.Ct.at 2219

248 *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.").

The majority's decision in *Carpenter* was supported by tech firms[249] and hailed as a victory of privacy by advocacy groups.[250] Others remained more cautious.[251] Professor Susan Freiwald and former Magistrate Judge Stephen Smith considered it an achievement that the *Carpenter* Court "significantly narrowed the [third-party] doctrine's scope,"[252] and that it "mark[ed] the first time the Court ha[d] explicitly announced the possibility of reasonable expectations of privacy in records stored with a third party."[253] They also pointed out that it had been ten years since the issue was raised by magistrate judges and called for guidance; and twenty-four years since Congress had signaled that CSLI data is entitled to greater legal protection.[254]

There are even more reasons to be cautious. The Court was explicit about its ruling being limited to seven days of historical CSLI;[255] it even refused to extend

---

249 Brief for Technology Companies as *Amici Curiae* in Support of Neither Party, No. 16-402, Aug. 14, 2017, 2017 WL 3601390 (U.S.) (Appellate Brief filed by Airbnb, Apple, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest Labs, Oath, Snap, Twitter, and Verizon). The brief stated, "Rigid rules such as the third-party doctrine and the content/non-content distinction made 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."

250 Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J. L. & TECH. 357 (Spring 2019); Nicholas A. Kahn-Fogel, Katz, Carpenter, *and Classical Conservatism*, 29 CORNELL J. L. & PUB. POL'Y 95 (Fall 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 (2019); Alan Z. Rozenshtein, *Fourth Amendment Reasonableness after* Carpenter, 128 YALE L.J. F. 943 (Apr. 2019). Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011) (Special Feature: Cyberlaw); 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 (Spring 2012); Christopher J. Borchert, Fernando M. Pinguelo & David Thaw, *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36 (2014).

251 Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205 (Nov. 2018) (The Supreme Court 2017 Term: Comments).

252 *Id*. at 224.

253 *Id*. at 226.

254 *Id*. at 231.

255 *Carpenter*, 138 S.Ct.at 2220. The majority expressly stated:

> 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

it to real-time CSLI. Other issues would have to wait for another day in court. The piecemeal approach is perhaps necessary—after all, the *Carpenter* majority was only a five-to-four weak majority and it does undercut the Court's function as a constitutional court guided by principles. But even this piecemeal approach is not guaranteed. Since 2018, Justice Kennedy has been replaced by Justice Brett Kavanaugh, and Justice Ginsburg by Justice Amy Coney Barrett. With the current configuration of the Supreme Court, the future of the *Carpenter* revolution seems uncertain. One possible path for the Court is to roll back the *Carpenter* decision, as the judges did in *Burger*. From the dissenting opinions, Justices Thomas, Alito, and Gorsuch all believed that the legislature is in a better position to make policy decisions, so courts should exercise "caution."[256] From this perspective, the *Carpenter* ruling shows how entrenched the surveillance state is in the United States.

2. Subscriber Information and Internet Protocol (IP) Addresses

Anonymity in cyberspace was both celebrated and feared in the early stages of the Internet,[257] but now it has become illusory in surveillance capitalism.[258] It turns out that every computer or device we use has a unique digit number called the Internet Protocol (IP) address that identifies the device. Your Internet Service Provider (ISP) has it, your cell phone company has it, as does Google if you use the Chrome browser and Apple if you use Safari. The government wants to obtain IP addresses, and the only sources for this information are service providers and digital platforms. In *United States v. Hambrick*,[259] police in New Hampshire found a suspect named "Blowuinva" in an online chat room who was enticing teenagers to have sex with him. To find the true identity of "Blowuinva," police served a subpoena on the ISP, which complied by providing

---

location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.

256 *Id.* at 2223 (Kennedy, J., dissenting, joined by Thomas, J., and Alito, J.) (stating "In § 2703(d) Congress weighed the privacy interests at stake and imposed a judicial check to prevent executive overreach. The Court should be wary of upsetting that legislative balance and erecting constitutional barriers that foreclose further legislative instructions."); *Id*. at 2265 (Gorscuh, J., dissenting) (arguing for the positive law model—which meant that the court should look for positive law for guidance on the social norms on issues like privacy). On the positive law model, *see*, William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821 (May 2016); Nicholas A. Kahn-Fogel, Katz, Carpenter, *and Classical Conservatism*, 29 CORNELL J. L. & PUB. POL'Y 95 (Fall 2019).

257 Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639 (May 1995) (Symposium: Emerging Media Technology and the First Amendment); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L. J. 869 (Summer 1996) (The Randolph W. Thrower Symposium: Legal Issues in Cyberspace: Hazards on the Information Superhighway).

258 SCHNEIER, *supra* note 8, at 53 ("In the age of ubiquitous surveillance, where everyone collects data on us all the time, anonymity is fragile.").

259 United States v. Hambrick, 55 F.Supp.2d 504, 505-06 (W.D. Va. 1999), *aff'd* 225 F.3d 656 (4th Cir. 2000) (unpublished opinion).

the defendant's name, address, credit card number, e-mail address, telephone numbers, and the fact that the defendant's account was connected to the web at the IP address. The federal district court ruled that "[f]or Fourth Amendment purposes, this court does not find that the ECPA has legislatively determined that an individual has a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection."[260] This was soon followed by similar rulings by the federal district court in Kansas[261] and the Sixth Circuit.[262]

After the Patriot Act, the first major federal court decision was *United States v. Forrester*.[263] Here, the Court considered the legality of a computer surveillance technique called "mirror port," involving a pen register analogue that was installed on the defendant's ISP connection facility in San Diego. This enabled the government to learn the to/from addresses of the defendant's email messages, the IP addresses of websites he visited, and the total volume of information sent to or from his account.[264] Having noted this "as a matter of first impression,"[265] the Ninth Circuit concluded that "this surveillance was analogous to the use of a pen register that the Supreme Court held in *Smith v. Maryland* did not constitute a search for Fourth Amendment purposes."[266] The Ninth Circuit gave two reasons for this conclusion: First, the third-party element. Like the telephone users in *Smith*, email and Internet users have no expectation of privacy in the addressing information "because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[267] Second, addressing information, like the phone numbers in *Smith*, does not reveal contents; "the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here."[268]

The Ninth Circuit conceded that "[a]t best, the government may make educated guesses about what was said in the messages or viewed on the websites based on its knowledge of the email to/from addresses and IP addresses—but this is no different from speculation about the contents of a phone conversation on the

---

260 *Id*. at 507.

261 United States v. Kennedy, 81 F.Supp.2d 1103, 1110 (D. Kan. 2000) ("Defendant's constitutional rights were not violated when [ISP] divulged his subscriber information to the government.").

262 *See* Guest v. Leis, 255 F.3d 325 (6th Cir. 2001).

263 United States v. Forrester, 512 F.3d 500 (9th Cir. 2008), amend'g 495 F.3d 1041 (9th Cir. 2007); Schuyler Sorosky, Comment, United States v. Forrester: *An Unwarranted Narrowing of the Fourth Amendment*, 41 LOY. L. A. L. REV. 1121 (Spring 2008).

264 Forrester, 512 F.3d at 505.

265 *Id*. at 510 ("Neither this nor any other circuit has spoken to the constitutionality of computer surveillance techniques that reveal the to/from addresses or email messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account.").

266 *Id*. at 504 (citation omitted).

267 *Id*. at 510.

268 *Id*.

basis of the identity of the person or entity that was dialed."[269] The Court made it clear that "our holding extends only to these particular techniques and does not imply that more intrusive techniques or techniques that reveal more content information are also constitutionally identical to the use of a pen register."[270]

The Tenth Circuit quickly came to the same conclusion in *United States v. Perrine*.[271] In this case, police got tips about a suspect in Yahoo!'s chat room; police only had the suspect's IP address. They applied for and obtained a disclosure order under 18 U.S.C. § 2703(d) to Yahoo!, for the latter to provide subscriber information. The Tenth Circuit noted, "[e]very federal court to address this issue has held that subscriber information provided to an Internet provider is not protected by the Fourth Amendment's privacy expectation."[272] Other circuit courts followed this position.[273]

---

269 Forrester, 512 F.3d at 510.

270 *Id*. In 2019, the Ninth Circuit was asked to revisit the position in *Forrester* in light of *Carpenter*. In its unpublished opinion, the Ninth Circuit rejected the request, noting *Carpenter*'s narrow holding, United States v. VanDyck, 776 Fed. App'x 495 (9th Cir. 2019). More recently, the Ninth Circuit was asked again to extend *Carpenter* to subscriber information and IP addresses in United States v. Rosenow, No. 20-50052, D.C. No. 3:17-cr-03430-WQH-1, the Ninth Circuit, Oct. 3, 2022, amending and superseding United States v. Rosenow, 33 F.4th 529 (9th Cir. 2022). The Ninth Circuit declined the invitation. Again, the Ninth Circuit declined unanimously (the only dissenting opinion was on a different issue). The Court rather confirmed its rationale in *Forrester* when it stated: "Specifically, in *Forrester* we analogized IP addresses and email to/from lines to the 'information people put on the outside of mail,' which the Supreme Court has long held can be searched without a warrant . . . therefore, there is no legitimate expectation of privacy in such information. This basic information differs from the content of email messages and other private communications, which are analogous to the sealed contents of mail, which the government does need a warrant to search."

271 United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008).

272 *Id*. at 1204.

273 *See* United States v. Bynum, 604 F.3d 161 (4th Cir. 2010) (FBI obtained defendant's IP address and other subscriber information from Yahoo! via an administrative subpoena); United States v. Christie, 624 F.3d 558, 573–74 (3rd Cir. 2010) (FBI acquiring defendant's IP address from ISP was not a violation of the Fourth Amendment because he had no expectation of privacy in his IP address); United States v. Wheelock, 772 F.3d 825 (8th Cir. 2014) (police obtained defendant's subscriber information from Comcast, the ISP, via an administrative subpoena); United States v. Caira, 833 F.3d 803 (7th Cir. 2016) (DEA obtained defendant's IP address and other subscriber information from Comcast, the ISP, and subscriber information from Microsoft, both via an administrative subpoena); United States v. Weast, 811 F.3d 743 (5th Cir. 2016) (police obtained IP address and subscriber information from ISP via a subpoena); United States v. Ulbricht, 858 F.3d 71 (2nd Cir. 2017).

The narrow holding of *Carpenter* became the new guidance for circuit courts.[274] In *United States v. Contreras*,[275] a case decided three months after *Carpenter*, the Fifth Circuit found that an IP address "falls comfortably within the scope of the third-party doctrine."[276] This may pose some challenges to those who read *Carpenter* as a revolution of privacy protection law. It is even clearer in cases where courts try to delimit the scope of *Carpenter* itself. In *United States v. Soybel*,[277] law enforcement installed a pen register to obtain the IP address of the defendant; and the defendant relied on *Carpenter* to move for suppression of that evidence. The Seventh Circuit ruled that "*Carpenter* has no bearing on the government's collection of IP-address data from a suspect's internet traffic."[278]

In state courts, *Carpenter* may have a similar effect. Prior to *Carpenter*, the New Jersey Supreme Court had ruled that the New Jersey Constitution protects subscriber information.[279] A couple of years later, the New Hampshire Supreme Court, however, decided to "join the overwhelming majority of federal and state courts" in holding that the New Hampshire Constitution does not protect a reasonable expectation of privacy in subscriber information.[280] The Supreme Court of Vermont quickly followed suit.[281] After *Carpenter*, the Arizona Supreme Court continued this direction in *State v. Mixton*.[282] It found guidance in a narrow reading of *Carpenter*:

> *Carpenter* expressly preserves existing applications of *Smith* and *Miller* and its logic does not extend its exception to the third-party

---

274 *See* United States v. Contreras, 905 F.3d 853 (5th Cir. 2018) (Homeland Security agents obtained subscriber information from Kik, a mobile messaging application, and IP addresses from Frontier Communications, the ISP, both via grand jury subpoenas); United States v. Wellbeloved-Stone, 777 Fed. Appx 605 (4th Cir. 2019) (agents of Immigration and Customs Enforcement obtained IP address and internet and email subscriber information via summonses); United States v. Hood, 920 F.3d 87 (1st Cir. 2019) (Homeland Security agents obtained subscriber information from Kik, a social media app via an Emergency Disclosure Request under the SCA, 18 U.S.C. § 2702); United States v. Morel, 922 F.3d 1 (1st Cir. 2019) (New Hampshire police obtained IP address from Comcast via a subpoena); United States v. Trader, 981 F.3d 961 (11th Cir. 2020) (Homeland Security agents obtained IP addresses, email address from Kik and subscriber information from Comcast via an Emergency Disclosure Request).

275 United States v. Contreras, 905 F.3d 853 (5th Cir. 2018).

276 *Id*. at 857.

277 United States v. Soybel, 13 F.4th 584 (7th Cir. 2021).

278 *Id*. at 592.

279 *See* State v. Reid, 194 N.J. 386, 945 A.2d 26 (2008) (in a computer theft case, law enforcement relied on a deficient municipal subpoena to obtain from Comcast suspect's IP address); James C. Jones, Jr., *Searches and Seizures—New Jersey Recognizes an Individual's Privacy Interest in the Subscriber Information Relayed to an Internet Service Provider*, 40 RUTGERS L.J. 939 (Summer 2009).

280 State v. Mello, 27 A.3d 771, 775 (N.H. 2011).

281 State v. Simmons, 2011 VT. 69, 27 A.3d 1065 (Vt. 2011).

282 State v. Mixton, 250 Ariz. 282, 478 P.3d 1227 (Ariz. 2021).

> doctrine for CSLI information to IP addresses and ISP subscriber information.[283]

Similarly, in a Pennsylvania case, *Commonwealth v. Dunkins*,[284] the Supreme Court considered location information revealed by wireless internet network (WiFi) different from CSLI revealed by cell towers; therefore, the *Carpenter* exception did not apply.

In sum, in subscriber information and IP addresses, it is obvious that the *Carpenter* ruling did not lead to a revolution in offering a stronger protection of privacy. Many courts found guidance in *Carpenter,* but in the opposite direction.

3. Stored Emails

If CSLI, subscriber information, and an IP address can be comfortably categorized as traffic data, which is different than content data, it seems obvious that content data would be better protected. Whether emails are protected by the Fourth Amendment, however, remains unclear. One early case that confronted this issue was *Theofel v. Farey-Jones*,[285] where the defendant accessed the plaintiffs' emails via an invalid subpoena to NetGate, the internet service provider (ISP). Plaintiffs then moved to quash the subpoena. In dicta, the Ninth Circuit stated, "[t]he false subpoena caused disclosure of documents that otherwise would have remained private; it effected an 'invasion . . . of the specific interest that the [statute] seeks to protect.'"[286] In *Quon v. Arch Wireless*,[287] there was an investigation of employees' usage of pagers after the City of Ontario obtained text messages from the ISP. Arch Wireless employees filed suit against the ISP and the City, alleging violation of the SCA and the Fourth Amendment. On the Fourth Amendment issue, the Ninth Circuit found "users do have a reasonable expectation of privacy in the content of their text messages vis-à-vis the service provider,"[288] and that the search was not reasonable in scope.[289] The United States Supreme Court reversed the ruling after finding the search was reasonable.[290] But it decided not to touch on the issue of whether the expectation of privacy was reasonable or not; rather, it simply assumed that Quon had a reasonable expectation of privacy.[291]

One month after the *Quon* ruling, the Eleventh Circuit in *Rehberg v. Paulk* took the Supreme Court's position as a "marked lack of clarity in what privacy

---

283 *Id*. at 1234.

284 Commonwealth v. Dunkins, 263 A.3d 247 (Pa. 2021).

285 Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004), *superseding an earlier opinion*, Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003).

286 Theofel, 359 F.3d at 1074.

287 Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008), *rev'd in* City of Ontario v. Quon, 560 U.S. 746 (2010).

288 *Id*. at 905.

289 *Id*. at 908–09.

290 City of Ontario v. Quon, 560 U.S. 746 (2010).

291 *Id*. at 757.

expectations as to content of electronic communications are reasonable."[292] The Eleventh Circuit therefore concluded that the constitutional right in email content was not clearly established.[293] Two years later, in 2012, an unanimous Supreme Court of the United States affirmed the decision based on other legal issues, without any reference to the question of email or subpoena.[294] Five months after the Eleventh Circuit's ruling, the same question was raised in the Sixth Circuit in *Warshak v. United States*.[295] Here, after being convicted of a number of crimes, the defendant, Steven Warshak moved to exclude thousands of emails that the government obtained from his ISPs, including NuVox Communications. The government used a § 2703(b) subpoena and an *ex parte* court order under § 2703(d) to compel NuVox to turn over the emails. Warshak did not receive notice on either the subpoena or the court order until one year later. The Sixth Circuit concluded that:

> The government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause. Therefore, because they did not obtain a warrant, the government agents violated the Fourth Amendment when they obtained the contents of Warshak's emails. Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.[296]

In 2014, four years after the Sixth Circuit's decision, the United States Supreme Court simply denied *certiorari*.[297] The Supreme Court has not provided any guidance on this issue since, which is surprising given that lower courts have been buried in questions about stored emails.[298]

---

292 Rehberg v. Paulk, 611 F.3d 828, 844 (11th Cir. 2010), *aff'd* Rehberg v. Paulk, 566 U.S. 356 (2012).

293 *Id*. at 846.

294 Rehberg v. Paulk, 566 U.S. 356 (2012).

295 Warshak v. United States, 631 F.3d 266 (6th Cir. 2010).

296 *Id*. at 288. The Sixth Circuit's view reflected views from scholars, *e.g*., Susan Freiwald & Patricia L. Bellia, *The Fourth Amendment Status of Stored E-Mail: The Law Professors' Brief in Warshak v. United States*, 41 U.S.F. L. REV. 559 (Spring 2007) (Symposium: Companies Caught in the Middle); Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121 (2008) (Law in a Networked World); Courtney M. Bowman, *A Way forward after Warshak: Fourth Amendment Protections for E-Mail*, 27 BERKELEY TECH. L.J. 809 (2012).

297 Warshak v. United States, 574 U.S. 1000 (2014); Joy L. Backer, Note, *Stop Waiting on the World to Change: Compelled Disclosure of Email Content under the Stored Communications Act*, 48 SUFFOLK U. L. REV. 379 (2015).

298 Paul S. Grewal, a federal Magistrate Judge, wrote in 2014, "[b]y virtue of the government's significant interest in the stored email of service providers, it is the . . . the Stored Communications Act, that captures the lion's share of the court's attention." *In the Matter of* the Search Warrant for: [Redacted]@Hotmail.com, 74 F.Supp.3d 1184, 1185 (N.D. Cal. 2014).

In *Walker v. Coffey*,[299] the Third Circuit noted that "at present *Warshak* remains closer to a lonely outlier than to a representation of consensus."[300] Here, Walker was an employee of Pennsylvania State University, which handed her work emails over to police upon an invalid subpoena. Walker filed a lawsuit alleging violation of her Fourth Amendment rights. The Third Circuit concluded that "we would be hard put to find that Walker enjoyed a clearly established right to privacy in the content of her work emails."[301] On the distinction between metadata and content, the Third Circuit asserted: "that distinction is not dispositive, as content is not uniformly protected."[302] The key, according to the Third Circuit, was that Walker's work email was controlled and operated by a third-party, Penn State: "for the purposes of the Fourth Amendment, the emails were subject to the common authority of Walker's employer."[303] Following the third-party doctrine, "Walker did not enjoy any reasonable expectation of privacy vis-à-vis Penn State, and Penn State could independently consent to a search of Walker's work emails."[304] Two years later, the *Walker* case came to the Third Circuit for the second time, on the question whether the SCA protected the privacy of Walker's work emails.[305] The Court remained steadfast and found no violation of SCA Section 2703 since Penn State's production of Walker's emails was voluntary.[306]

In the age of cloud computing, the third-party doctrine insisted by the courts is a powerful tool that enables law enforcement to have access to contents of communication with little constraints by the Fourth Amendment or the SCA.

B. Asymmetric Access

Without Fourth Amendment protection, the SCA provides the basic legal framework for electronic communications. The main components of this framework include the general prohibition under § 2702(a), and exceptions under § 2703(b) and § 2703(c). Once it is decided that an exception to the general prohibition applies, disclosure can be enforced under state law.[307] This Section claims that SCA greatly privileges government access to digital data while severely undercutting the ability of criminal defendants to take advantage of the same.[308]

---

299 Walker v. Coffey, 905 F.3d 138 (3rd Cir. 2018) (Walker I).

300 *Id.*, at 148.

301 *Id*.

302 *Id*.

303 *Id.*, at 149.

304 Walker I, 905 F.3d 138 at 149.

305 Walker v. Coffey, 956 F.3d 163 (3rd Cir. 2020) (Walker II).

306 *Id*. at 167.

307 Facebook, Inc. v. Superior Court (Hunter), 233 Cal.Rptr.3d 77, 417 P.3d 725, 751 (Cal. 2018) (discussing Negro v. Superior Court, 230 Cal.App.4th 879, 179 Cal.Rptr.3d 215 (2014) with approval).

308 *See* generally Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. REV. 212 (May 2021); Jenia I. Turner, *Managing Digital Discovery in Criminal Cases*, 109 J. CRIM. L. & CRIMINOLOGY 237 (Spring 2019);

Just like the primary interest in surveillance capitalism is profits, not users; the surveillance state's primary service is to the state, not its citizens.

1. General Prohibition

The general prohibition under § 2702(a) provides: Except as provided in subsection (b) or (c), the electronic communication service provider "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[309] "Contents" under the SCA does not include metadata regarding characteristics of messages; thus, the SCA general prohibition does not include referrer header information.[310]

In criminal cases, the typical request is to subpoena the victim's social media. In *Facebook, Inc. v. Wint*,[311] Daron Wint was charged with murder in the Superior Court of District of Columbia. Before trial, he filed an *ex parte* motion asking the trial court to authorize defense counsel to serve subpoena *duces tecum* on Facebook for records, including the contents of communications relating to certain accounts. Facebook refused and was held in civil contempt. The D.C. Court of Appeals concluded, "[c]riminal defendants' subpoenas were not included by Congress in the list of exceptions, which tends to support a conclusion that Congress did not intend to permit disclosure in response to criminal defendants' subpoenas."[312] In Oregon, *State v. Bray* considered a similar issue.[313] Here, defendant, who was charged with rape in Oregon state court, sought to compel production of the victim's digital data from Google in order to prove sex was consensual. The trial court granted the defendant's motion, and the state served a subpoena duces tecum to Google. Google, however, refused to comply.

In California, the Penal Code allows officials and persons—including defense counsel—to issue criminal subpoenas.[314] A criminal subpoena does not command, or even allow, the recipient to provide materials directly to the requesting party; instead, the materials must be given to the superior court for its review so as

---

Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569 (Winter 2007) (Symposium: Technical Change and the Evolution of Criminal Law).

309 18 U.S.C. § 2702(a)(1) (2018).

310 *In re* Zynga Privacy Litigation, 750 F.3d 1098, 1106 (9th Cir. 2014) ("the term 'contents' refer to the intended message conveyed by the communication and does not include record information regarding the characteristics of the message that is generated in the course of the communication."); *In re* Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589, 609 (9th Cir. 2020) (affirming trial court's dismissal of claims based on alleged disclosing of "referrer header" information).

311 Facebook, Inc. v. Wint, 199 A.3d 625 (D.C. 2019).

312 *Id.*, at 632.

313 State v. Bray, 363 Or. 226, 422 P.3d 250 (Or. 2018).

314 Cal. Penal Code § 1326(a) (West 2008).

to decide its relevance and use.[315] In *Facebook v. Superior Court (Touchstone)*,[316] an attempted murder case, the defendant, Lance Touchstone, sought the victim's Facebook communications, believing that the Facebook account might provide exculpatory evidence helpful in preparing for trial. Facebook moved to quash the subpoena, based on the general prohibition in the SCA. The Supreme Court of California did not directly address the issue of whether the SCA permitted disclosure under such a subpoena. The Court did rule, however, that even if disclosure is permitted, the requesting party must show good cause when countered by Facebook's motion to quash, and the trial court review relevant factors.

The general prohibition applies equally to civil cases. In a copyright dispute, *Crispin v. Christian Audigier, Inc.*,[317] the defendants served subpoenas *duces tecum* on Facebook and MySpace, seeking all communications between the plaintiff and a third-party, including all communications referred to or related to the defendant. Plaintiff filed an *ex parte* motion to quash the subpoenas. The federal court for the Central District of California granted the motion to quash the subpoenas because, among the statute's exceptions, "[t]he statute does not mention service of a civil subpoena *duces tecum*."[318] The federal district court in California followed the language of East Virginia's federal district court closely in deciding a contract dispute. When State Farm, an insurance company, subpoenaed American Online (AOL) for documents the federal court ruled that, "AOL, a corporation that provides electronic communication services to the public, may not divulge the contents of the [subpoenaed] electronic communications to State Farm because the statutory language of the [SCA] does not include an exception for the disclosure of electronic communications pursuant to civil discovery subpoenas."[319]

2. Exception: Intended Recipient

The exception under § 2702(b)(1) provides: A provider described in subsection (a) may divulge the contents of a communication "to an addressee or intended recipient."[320] In *Facebook, Inc. v. Pepe*,[321] the defendant, James Pepe, was charged with shooting Marquette Brown. Before trial, Pepe requested court

---

315 Cal. Penal Code § 1326(c) (West 2008).

316 Facebook, Inc. v. Super. Ct. of San Diego, 471 P.3d 383 (Cal. 2020).

317 Crispin v. Christian Audigier, Inc., 717 F.Supp.2d 965 (C.D. Cal. 2010).

318 *Id.*, at 975; *see*, *also*, Ryan A. Ward, Note, *Discovering Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J. L. & TECH. 563 (Spring 2011).

319 *In re* Subpoena Duces Tecum to AOL, LLC. No. 1:07mc34 (GBL), 550 F.Supp.2d 606, 611 (E.D. Va. 2008). *See*, *also*, Viacom International Inc. v. YouTube, Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) ("Defendants are prohibited by the [SCA] from disclosing the private videos and the data which reveal their contents because … [SCA] § 2702 contains no exception for disclosure of such communications pursuant to civil discovery requests."); Federal Trade Commission v. Netscape Communications Corp., 196 F.R.D. 559 (N.D. Cal. 2000).

320 18 U.S.C. § 2702(b)(1) (2018).

321 Facebook, Inc. v. Pepe, 241 A.3d 248 (D.C. 2020).

authorization for an *ex parte* subpoena from social networking company Facebook, seeking communications from Brown's Instagram account to Pepe's account in order to support self-defense claims. Facebook refused and was held in civil contempt by the trial court. On appeal, Facebook filed a motion to quash the subpoena based on the SCA. Facebook argued that Pepe was not an "addressee or intended recipient" of Instagram messages because the message Brown sent expired and disappeared from the platform after twenty-four hours.[322] The D.C. Court of Appeals ruled that Pepe was clearly the recipient because "[t]he status of intended recipient does not depend on whether the recipient keeps the communication or whether the sender intended that it be preserved."[323]

3. Exception: Lawful Consent

The exception under § 2702(b)(3) provides: A provider described in subsection (a) may divulge the contents of a communication "with the lawful consent of the originator or an addressee or intended recipient."[324] In *Facebook, Inc. v. Superior Court (Hunter)*,[325] the defendants convicted in a murder trial served subpoenas *duces tecum* on Facebook, Instagram, and Twitter, seeking public and private communications from the social media accounts of the homicide victim and a prosecution witness. Social media providers moved to quash the subpoenas. According to the Supreme Court of California:

> [B]y virtue of section 2702(a), the Act generally and initially prohibits the disclosure of all (even public) communications—but that section 2702(b)(3)'s subsequent lawful consent exception allows providers to disclose communications configured by the user to be public.[326]

What are "communications configured by the user to be public?" According to the Supreme Court of California's reading of legislative history, "a communication is readily accessible to the general public if the . . . means of access [is] widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy."[327] The Court rejected the defendants' argument that implied consent to disclosure is established when a communication is configured by the user to be accessible to a "large group" of friends or followers.[328]

322 *Id.*, at 254–55.
323 *Id.*, at 255.
324 18 U.S.C. § 2702(b)(3) (2018).
325 Facebook, Inc. v. Super. Ct. (Hunter), 417 P.3d 725 (Cal. 2018).
326 *Id.*, at 743–44.
327 *Id.*, at 739.
328 *Id.*, at 746–49.

4. Exception: Government Entity

Under SCA § 2703(b)(1), "a governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication" by a search warrant, administrative subpoena, or a court order.[329] In one instance, a warrant was issued under the SCA authorizing the search and seizure of information associated with a specific web-based e-mail account.[330] Microsoft, the operator of this email service, moved to quash the search warrant on the grounds that the content was stored on a server located in Dublin, Ireland and that the federal courts were without authority to issue warrants for search and seizure of property outside the territorial limits of the United States.[331] The motion was denied by the Magistrate Judge in the Southern District of New York.[332] On appeal, the Second Circuit ruled in 2016 that the warrant violated the presumption against extraterritoriality.[333] As the case went to the Supreme Court of the United States in March 2018, Congress enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act),[334] expanding the SCA's global reach to information "within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[335] Shortly after this Act, the Supreme Court briefly declared the Microsoft case moot.[336]

Constitutional concerns have been raised that the SCA created an uneven playing field. In *United States v. Pierce* (2015),[337] the defendant, Melvin Colon, raised the issue, claiming that the SCA was unconstitutional because it provides a mechanism for the government to obtain stored content, without a comparable mechanism for criminal defendants.[338] The Second Circuit rejected Colon's claim, finding that he had "not shown any injury from the statute."[339]

---

329 18 U.S.C. § 2703(b)(1) (2019).

330 In the Matter of Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, 15 F.Supp.3d 466 (S.D.N.Y. 2014).

331 *Id.*

332 *Id.*

333 In the Matter of Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197 (2nd Cir. 2016), reh'g en banc denied, In the Matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation, 855 F.3d 53 (2nd Cir. 2017), vacated, United States v. Microsoft Corp., 138 S.Ct. 1186 (2018).

334 Consolidated Appropriations Act, 2018 Pub. L. 115-141, 132 Stat. 1213 (Mar. 23, 2018).*See*, also, Miranda Rutherford, *The CLOUD Act: Creating Executive Branch Monopoly over Cross-Border Data Access*, 34 BERKELEY TECH. L.J. 1177 (2019); Secil Bilgic, Note, *Something Old, Something New, and Something Moot: The Privacy Crisis under the CLOUD Act*, 32 HARV. J. L. & TECH. 321 (Fall 2018).

335 18 U.S.C. § 2713 (2018).

336 *United States v. Microsoft Corp.*, 138 S.Ct. 1186 (2018).

337 *United States v. Pierce*, 785 F.3d 832 (2nd Cir. 2015).

338 *Id.*, at 841.

339 *Id.*, at 842.

C. Secrecy

In its 2016 complaint filed with the federal district court for Western Washington, Microsoft alleged that "[o]ver a 20-month period ending in May 2016, federal courts issued more than 3,250 secrecy orders silencing Microsoft from speaking about the government's legal demands for Microsoft customers' data. Of those secrecy orders, nearly two-thirds contained no fixed end date."[340] There are no official numbers for the warrants or court orders issued because the Department of Justice does not keep them.[341] There are two kinds of secret orders. One is a nondisclosure order under 18 U.S.C. § 2705(b) of the Stored Communications Act, which prohibits a service provider from notifying subscribers of the existence of a search warrant.[342] The other is National Security Letters (NSLs), a counter-intelligence measure under 18 U.S.C. § 2709, which grants the Federal Bureau of Investigation the power to access subscriber information held by ISPs in secret.[343] Both measures deal with the relationship between service providers and the government entity requesting the information. This Section will focus on the § 2705(b) orders.

Microsoft noted in its complaint in 2016, "[a]s individuals and businesses have moved their most sensitive information to the cloud, the government has increasingly adopted the tactic of obtaining the private digital documents of cloud customers not from the customers themselves, but through legal process directed at online cloud providers like Microsoft."[344] However, as in the telegraph and telephone era, the government prefers obtaining the information in secret. According to Microsoft, "the government seeks secrecy orders under 18 U.S.C. § 2705(b) to prevent Microsoft from telling its customers (or anyone else) of the

---

340 First Amended Complaint for Declaratory Judgment, at ¶5, *Microsoft Corp. v. United States*, 2016 WL 3381727 (W.D. Wash. 2016) (No. 2:16-cv-00538-JLR) (Trial Pleading).

341 *See* The Electronic Communications Privacy Act: Providing Security and Protecting Privacy in the Digital Age, Hearing before the S. Committee on the Judiciary, 111th Cong., 2nd Sess., Sep. 22, 2010, Ser. No. J-111-109 [hereinafter, Senate Judiciary 2010 ECPA Hearing] (Associate Deputy Attorney General James A. Baker's response to questions submitted by Senator Russell D. Feingold).

342 18 U.S.C. § 2705 (1986).

343 *See generally*, 18 U.S.C. §2705; In re Search Warrant Issued to Google, Inc., 269 F.Supp.3d 1205 (N.D. Ala. 2017); In the Matter of the Search of Information Associated with Specified E-mail Accounts, 470 F.Supp.3d 285 (E.D.N.Y. 2019); Google LLC v. United States, 443 F.Supp.3d 447 (S.D.N.Y. 2020); Twitter, Inc. v. Barr, 445 F.Supp.3d 295 (N.D. Cal. 2020); In the Matter of the Search of Information Associated with E-mail Accounts, 468 F.Supp.3d 556 (E.D.N.Y. 2020). Rebecca Wexler, *Gags as Guidance: Expanding Notice of National Security Letter Investigations to Targets and the Public*, 31 BERKELEY TECH. L.J. 325 (2016, No.1); Rebecca Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, 124 YALE L.J. F. 158 (2014-2015); Andrew E. Nieland, Note, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1201 (Sep. 2007, No.6).

344 First Amended Complaint for Declaratory Judgment at ¶4, *supra* note 340.

government's demands."[345] Microsoft thus contended that § 2705(b) was unconstitutional under the First and Fourth Amendments.[346] In the same year, Microsoft was joined by Adobe and Google in challenging the constitutionality of indefinite duration of nondisclosure orders under the First Amendment in federal district courts across the United States west coast.[347]

In Microsoft's case, Judge James L. Robart laid the foundation for the First Amendment review of nondisclosure orders by recognizing that Microsoft had sufficiently alleged injury-in-fact and likelihood of future injury, which established the standing to sue;[348] that the nondisclosure orders constituted a content-based prior restraint, which subjected § 2705(b) to strict scrutiny review;[349] and that it violated the First Amendment because it was overbroad.[350] In March 2017, the federal district court in Central California dealing with Adobe's case came to a similar conclusion. In September 2017, the Federal District Court for Northern Alaska deciding Google's case agreed. Victories in the courtrooms led to a settlement with the Justice Department. On October 19, 2017, the DOJ issued a memorandum to United States attorneys and agents that directed their use of protective orders.[351] The memorandum required changes:

> (1) that prosecutors conduct an "individualized and meaningful assessment" regarding the need for non-disclosure orders before seeking one;[352]
> (2) that prosecutors should "tailor the application to include the available facts of the specific case and/or concerns attendant to the particular type of investigation;"[353] and
> (3) that "[b]arring exceptional circumstances, prosecutors filling § 2705(b) applications may only seek to delay notice for one year or less."[354]

---

345 *Id.*

346 Microsoft Corp. v. United States Department of Justice, 233 F.Supp.3d 887, 896 (W.D. Wash. 2017).

347 In the Matter of Search Warrant for [Redacted].com, 248 F.Supp.3d 970 (C.D. Cal. 2017) (Adobe's case); *In re* Search Warrant Issued to Google, Inc., 269 F.Supp.3d 1205 (N.D. Ala. 2017) (Google's case).

348 Microsoft Corp., 233 F.Supp.3d at 877, 899–903.

349 *Id.*, at 904–08; Al-Amyn Sumar, *Prior Restraints and Digital Surveillance: The Constitutionality of Gag Orders Issued under the Stored Communications Act*, 20 YALE J.L. & TECH. 74 (2018).

350 Microsoft Corp., 233 F.Supp.3d at 908–10.

351 Deputy Attorney General Rod Rosenstein, Memorandum for Heads of Department, Law Enforcement Components, Department Litigation Components, the Director, Executive Office for U.S. Attorneys, All United States Attorneys, Oct. 19, 2017, https://www.justice.gov/criminal-ccips/page/file/1005791/download [https://perma.cc/9D59-FXPC] (last accessed Jun. 16, 2021).

352 *Id.*, ¶ 1 at 2.

353 *Id.*, ¶ 2 at 2.

354 *Id.*, ¶ 4 at 2.

Microsoft and Google continued challenging nondisclosure orders in federal courts under the First Amendment.[355] In January 2020, the Third Circuit became the first federal circuit court that affirmed the First Amendment rulings.[356] After the 2017 Memorandum, however, all nondisclosure orders passed the First Amendment scrutiny without much difficulty. We now know that the Justice Department misused its power for political purposes by seeking data from Apple and Twitter[357] and was able to keep it secret under § 2705(b). Brad Smith, President of Microsoft, wrote in the *Washington Post*, "The government cannot justify secrecy in such probes." Smith emphasized, "[d]emocracy rests on a fundamental principle of government transparency. Secrecy should be the rare exception—not the rule."[358]

In sum, the symbiotic model of the surveillance state is characterized by the three aspects of the legal framework discussed above: limited constitutional constraint, asymmetric access to data, and secrecy. The popular view that data is power is only half right. Digital platforms, as powerful as they are, are forced to provide data to the surveillance state in a legal framework—the SCA—that privileges the latter. The Fourth Amendment was not designed to protect the surveillance state. The Supreme Court had stopped functioning as a constitutional court long before the arrival of the internet, and it does not look like it will resume that function soon. The United States can only be more entrenched in the symbiotic model in the near future.

D. Comparative Perspective

The global trend towards increased government access to data held by private companies is unmistakable.[359] Global digital platforms are receiving a

---

355 *In re* Search of Info. Associated with Specified E-mail Accts., 470 F.Supp.3d 285 (E.D.N.Y. 2019) (Microsoft); In re Search of Info. Associated with Specified E-mail Accts., 468 F.Supp.3d 556 (E.D.N.Y. 2020) (Microsoft); *Google LLC v. United States*, 443 F.Supp.3d 447 (S.D.N.Y. 2020) (Google).

356 In the Matter of the Application of Subpoena 2018R00776, 947 F.3d 148 (3rd Cir. 2020).

357 It was revealed in June 2021 by the *New York Times* that the Justice Department under President Donald J. Trump subpoenaed Apple for data from the accounts of Democrats on the House Intelligence Committee, aides and family members. *See* Katie Benner, Nicholas Fandos, Michael S. Schmidt & Adam Goldman, *Hunting Leakers, Justice Dep. Got Democrats' Data*, N.Y. TIMES, Jun. 11, 2021, A1. It was revealed by the *New York Times* that the Justice Department under the Trump administration tried to use grand jury subpoena on Twitter in order to identify a critic of Republican Representative Devin Nunes of California. *See* Charlie Savage, *Trump Justice Dept. Tried to Use Grand Jury to Identify Nunes Critic on Twitter*, N.Y. TIMES, May 17, 2021, https://www.nytimes.com/2021/05/17/us/politics/devin-nunes-twitter-justice-department.html (last accessed May 19, 2021).

358 Brad Smith, *The Secret Gag Orders Must Stop*, WASH. POST, Jun. 14, 2021, A21.

359 Ira S. Rubinstein, Gregory T. Nojeim & Ronald D. Lee, *Systematic Government Access to Private-Sector Data: A Comparative Analysis*, in BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 5 (Fred H. Cate & James X Dempsey eds.

growing number of requests for data from all over the globe.[360] This means the symbiotic model of the surveillance state is spreading throughout the globe, together with the internet and social media. However, despite law enforcement agencies in different countries using different legal instruments,[361] we can still detect some similarities and crucial differences.

In Canada, Australia, and New Zealand, in addition to warrants, "production orders" are available for law enforcement to compel the production of data. Unlike the administrative subpoena in the United States, a "production order" is under judicial supervision. In Canada, police can "request" an ISP to provide information in accordance with a federal statue called PIPEDA.[362] However, even if the ISP voluntarily discloses the subscriber data to the police, a "search" has occurred because a subscriber has a legitimate expectation of privacy.[363] In *R. v.*

2017) ("There has been an increase worldwide in government demands for data held by the private sector.").

360 CLOUD EVIDENCE GROUP, CRIMINAL JUSTICE ACCESS TO DATA IN THE CLOUD: COOPERATION WITH "FOREIGN" SERVICE PROVIDERS (2016) (Cloud Evidence Group is a research arm of the Cybercrime Convention Committee under the Council of Europe), available at: https://www.coe.int/en/web/cybercrime/ceg (last accessed Aug. 15, 2022).

361 Apple's *Transparency Report* (2021), for example, identified the following legal instruments used by different countries requesting data from Apple: Production Orders (Australia, Canada, New Zealand), Requisition or Judicial Rogatory Letters (France), Solicitud Datos (Spain), Ordem Judicial (Brazil), Auskunftsersuchen (Germany), Obligation de dépôt (Switzerland), 個人情報の開示依頼 (Japan), Personal Data Request (United Kingdom), *see*, APPLE TRANSPARENCY REPORT: GOVERNMENT AND PRIVATE PARTY REQUESTS (January 1 – June 30, 2021), available at: https://www.apple.com/legal/transparency/ pdf/requests-2021-H1-en.pdf (last access Aug. 15, 2022).

362 Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 ("PIPEDA"), regulates business handling of personal information. Under Section 7(3)(c.1) of the Act, a service provider "may disclose personal information without the knowledge or consent of the individual" if the disclosure is "made to a government institution or part of a government institution that has made a request for the information". Section 7(3)(c.1), PIPEDA.

363 R. v. Spencer, 2014 SCC 43, [2014] 2 SCR 212 (Sup. Ct. Canada). Here, the police identified the internet protocol (IP) address of a computer involved in child pornography. They then requested subscriber information pursuant to s.7(3)(c.1)(ii) of PIPEDA from the internet service provider (ISP). The ISP complied with the request by providing name, address and telephone number of the subscriber, which enabled the police to obtain a search warrant and eventually found the accused and had him convicted. Justice Cromwell, writing for a unanimous Supreme Court of Canada, stated that, "[a] request by a police officer that an ISP voluntarily disclose such information amounts to a search." *Id*., para.66. In R. v. Alsford, [2017] NZSC 42 (Mar. 29, 2017), the Supreme Court of New Zealand was asked to decide whether power consumption data voluntarily provided by utility companies upon police request constituted warrantless "search" therefore a violation of privacy. The Court largely followed the principles stated in R. v. Spencer and other Canadian cases but came to a different conclusion—the majority of the Court found the accused did not have reasonable of expectation of privacy because the power consumption data that the police obtained did not reveal intimate details of lifestyle and personal choices. *Id*., para.66.

Spencer, the Supreme Court of Canada does not consider the "request" under PIPEDA to create new search and seizure powers for the police,[364] and thus signals a strong preference for the police to go through judicial approval for a "production order."[365] A "production order" is issued by a Crown Court judge, based on reasonable grounds to believe, a standard lower than that for a search warrant.[366] Similarly, in Australia, a federal police officer investigating a serious offense may apply to a judge for a "notice" to produce documents.[367] A "notice to produce," once issued, creates a legal duty,[368] whereby failure to comply would be an offense.[369] In New Zealand, a "production order" regime was created in 2012 by the Search and Surveillance Act.[370] The "production order" is issued by a judge, justice of the peace, or a magistrate,[371] based on "reasonable grounds."[372] In general, a "production order" in Commonwealth countries reflects a slightly higher level of judicial control over law enforcement's access to data than an administrative subpoena in the United States.

Some other countries, however, adopt legal instruments more akin to the administrative subpoena in the United States. In the United Kingdom, the Investigatory Powers Act 2016 ("IPA") regulates data sharing with law

---

364 R. v. Spencer, 2014 SCC 43, para. 71 (". . . neither s. 487.014(1) of the Criminal Code, nor PIPEDA creates any police search and seizure powers . . .") (Justice Cromwell).

365 *Id*., para. 49 ("In this case . . . it seems clear that the police had ample information to obtain a production order requiring [the ISP] to release the subscriber information corresponding to the IP address they had obtained.") (Justice Cromwell).

366 R. v. Vice Media Canada, Inc., 2018 SCC 53, [2018] 3 S.C.R. 374 (Sup. Ct. Canada) (upholding an ex parte production order obtained by police on a media organization and its journalist); R. v. West, 2020 ONCA 473 (C.A. Ont., July 22, 2020) (on the legal standards for a judge to issue production order under s. 487.014 of the Criminal Code in a child pornography case where the police obtained a production order); R. v. Bykovets, 2022 ABCA 208 (C.A. Alb., Jun. 13, 2022) (the police having obtained production order on ISP in seeking subscriber information, therefore the case was distinguishable from R. v. Spencer).

367 § 3ZQO of Crimes Act 1914, No. 12, 1914 (Cth) (Australia). Dan Jerker B. Svantesson & Rebecca Azzopardi, *Systematic Government Access to Private-Sector Data in Australia*, in BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 221-40 (Fred H. Cate & James X Dempsey eds. 2017).

368 Sect. 3ZQR, Crimes Act 1914 (Cth).

369 Sect. 3ZQS, Crimes Act 1914 (Cth).

370 Search and Surveillance Act 2012, Public Act 2012, No.24, Apr. 5, 2012, Subpart 2 of Part 3 (Enforcement Officers' Powers and Orders). Justice Arnold noted in R. v. Alsford, [2017] NZSC 42 (Mar. 29, 2017), "[p]rior to the enactment of sub-pt 2 of pt 3 of the Search and Surveillance Act, there was no production order regime generally available to police to facilitate the investigation of criminal offences." *Id*., para.18.

371 § 3, Search and Surveillance Act 2012 (definition of "issuing officer").

372 § 72, Search and Surveillance Act 2012 (Conditions for Making Production Order). Justice Arnold noted in R. v. Alsford that the Law Commission, which recommended introducing the regime, "conceived of the production orders as an 'alternative to search warrants,' with the same essential requirements. The Commission specifically rejected having a lower threshold than applied to search warrants, such as reasonable grounds to suspect that the information sought would assist in the investigation of an offence." R. v. Alsford, [2017] NZSC 42, para.18 (citations omitted).

enforcement.[373] Under the IPA, law enforcement investigating a "serious crime" can seek an "authorization" from a "designated senior officer," [374] or an Investigatory Powers Commissioner, [375] rather than from a judge. After the authorization, the law enforcement officer can serve a notice to service providers,[376] and the notice creates an enforceable legal duty.[377] Similarly, in Ireland, according to a recently amended law,[378] a request for disclosure of data can be made by a member of Garda Síochána (national police service) holding a rank of superintendent or higher.[379] Under Ireland's framework, judicial approval is not required. In France, an officer of the judicial police—the French criminal law enforcement—may order a service provider to produce documents or data relevant to an inquiry in progress.[380] Compliance here is a legal duty.[381] If it is a preliminary investigation, a public prosecutor must grant specific authority to the judicial police to proceed with the data request.[382] In Germany, the Code of Criminal Procedure allows law enforcement and public prosecutors to have access to certain data with a judge's approval.[383] Since 2004, Section 113 of the Telecommunication Act (TKG) required service providers to provide certain subscriber data to law

---

373 Investigatory Powers Act 2016, 2016, c. 25 (Nov. 29, 2016), as amended by the Data Retention and Acquisition Regulations 2018, 2018 No. 1123 (Oct. 31, 2018), and interpreted by Home Office, Communications Data: Code of Practice (Nov. 2018). The IPA amended the Regulation of Investigatory Powers Act 2000 ("RIPA"), 2000, c. 23 (Jul. 28, 2000). Tristan Goodman, *The Investigatory Powers Act 2016: A Victory for Democracy and the Rule of Law?* 2018 BRISTOL L. REV. 2-26 (2018).

374 Section 61(1) of IPA, *Id.*

375 Section 60A of IPA, inserted in Regulation 5 of the Data Retention and Acquisition Regulations 2018, *supra* note 373.

376 Section 61(4)(c) of IPA, *supra* note 373.

377 IPA, *supra* note 373, at § 66.

378 Communications (Retention of Data) (Amendment) Act 2022, No. 25 of 2022 (Jul. 21, 2022) (Ireland), amending the Communications (Retention of Data) Act 2011, No.3 of 2011 (Jan. 26, 2011) (Ireland) (hereinafter, the Act of 2022). The 2022 amendment was a response to the ruling of the Court of Justice of the European Union in the *G.D.* case, *infra* note 394.

379 § 6, Act of 2022, *Id.*

380 Art. 60-1, French Code of Criminal Procedure. Winston J. Maxwell, *Systematic Government Access to Private-Sector Data in France*, in BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 49-60, at 51 (Fred H. Cate & James X Dempsey eds. 2017).

381 Art. 60-2, French Code of Criminal Procedure.

382 Art. 77-1-1, French Code of Criminal Procedure; Winston J. Maxwell, *supra* note380, at 51.

383 §§ 100g(2), 100j, and 100k, German Code of Criminal Procedure (StPO), (last amended on Mar. 25, 2022); Federal Law Gazette I, p.571, English translation available at https://dejure.org/gesetze/StPO (last access Aug. 20, 2022). Paul M. Schwartz, *Systematic Government Access to Private-Sector Data in Germany*, in BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA 61-90 (Fred H. Cate & James X Dempsey eds. 2017); Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L.J. 751 (2002-2003) (Symposium: Enforcing Privacy Rights).

enforcement and other public authorities if it is necessary for the prosecution of crimes.[384] In January 2012, the German Federal Constitutional Court (BVerfG) found Section 113 partially unconstitutional, for lacking statutory framework on access to data.[385] In May 2020, the Federal Constitutional Court, again, found Section 113 of TKG unconstitutional for having failed to pass the proportionality test.[386] Specifically, the court believed that matching subscriber data to IP addresses "falls within the scope of protection of Article 10(1) GG [the German Basic Law]."[387] The Court found, as a result, that even though it serves legitimate purposes, Section 113 did not satisfy the requirements of proportionality.[388] Using a metaphor of "double door," the Court emphasized that more control of data access—the second door—was required.[389] The Court was clearly conscious of the scenario where the state authorities use data from service providers for surveillance purposes.[390] In its 2020 ruling, the German Federal Constitutional Court did not

---

384 Sec. 113 of Telecommunication Act (TKG), of Jun. 22, 2004. TKG was last amended on Jun. 23, 2021, *infra* note 392. When TKG was first legislated in 1996, the data sharing regime was under Sec. 90 (Information Requests from Security Authorities), TKG, Jul. 25, 1996.

385 BVerfG, Order of the First Senate of Jan. 24, 2012, 1 BvR 1299/05 (Subscriber Data I), English translation available at the German Federal Constitutional Court website at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2012/01/rs20120124_1bvr129905en.html (last access Aug. 20, 2022).

386 BVerfG, Order of the First Senate of 27 May 2020, 1 BvR 1873/13, 1 BvR 2618/13 (Subscriber Data II), English translation available at the German Federal Constitutional Court website at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200527_1bvr187313en.html (last access Aug. 20, 2022). Also, Melissa Eddy, *German Police Have Too Much Access to People's Data, Court Rules*, N.Y. TIMES, Jul. 18, 2020, A11. By contrast, after Subscriber Data I, two German nationals challenged Sec. 113 at the European Court of Human Rights without success, *see*, Breyer v. Germany (Application No. 50001/12), Judgment, ECtHR (Fifth Section), Sept. 7, 2020.

387 Subscriber Data II, *Id.*, para.99. Article 10(1) of the Basic Law provides: "The privacy of correspondence, posts and telecommunications shall be inviolable." English translation available at the German Federal Ministry of Justice website: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0058 (last access). Here the Federal Constitutional Court's position is similar to that of the Supreme Court of Canada in *R. v. Spencer*, 2014 SCC 43.

388 Subscriber Data II, *Id.*, para.127.

389 Subscriber Data II, *Id.*, para.163.

390 Subscriber Data II, *Id.*, para.130 (". . . it is impermissible to create a data pool independent of such purpose limitations and to let various state authorities make subsequent decisions on the use of such a data pool based on their needs and political discretion.")

call for prior judicial approval,[391] but pointed to a direction of more legislative and administrative control of data access in the near future.[392]

In sum, laws in Great Britain, Ireland, France, and Germany differ less from that in the United States in terms of judicial scrutiny on *access* to the data. However, on the European Union level, the Court of Justice of the European Union (CJEU) has been developing a more rigorous rule on data *retention* through a series of rulings based on Directive 2002/58.[393] The most recent in this line of cases is *G.D.*,[394] a review of Irish law referred to earlier. Setting limits on data retention is the EU's approach to regulate the symbiotic relationship between the surveillance state and the internet industry.

In Japan, Apple receives a steady number of data requests from the government as well.[395] With a larger population, the number of requests from the Japanese government in the first half of 2021, for example, is comparable to that in France.[396] LINE, a popular social media app in Japan, reports that 69% of the

---

391 Subscriber Data II, *Id.*, para.252 ("The constitutional principle of proportionality does not require prior review by an independent body, for example in the form of a warrant issued by a court."). Specifically, according to the Court, "[i]n respect of access to certain subscriber data determined on the basis of dynamic IP addresses . . . no prior judicial authorization is required, despite the increased weight of interference compared to obtaining general subscriber data." *Id*., para. 254.

392 In June 2021, the German Federal Diet (Bundestag) reshuffled regulatory framework by amending TKG and passing a new federal statute—Data Protection and Privacy of Telecommunication and Telemedia Services Act (TTDSG), Jun. 23, 2021 (BGBl. I S. 1982; 2022 I p.1045), took effect from Dec. 1, 2021. A revised Sec. 113 is now Sec. 174 of the Telecommunications Act (TKG), Jun. 23, 2021, BGB1 I 2021, 1858.

393 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 (Directive on privacy and electronic communications), OJ 2002 L 201, p. 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of November 25, 2009, OJ 2009 L 337, p.11. Since 2014, the CJEU has interpreted Article 15 of the Directive 2002/58 and brought constitutional limits on data retention: *Digital Rights Ireland v. Minister for Communications, Marine and Natural Resources and Others* (C-293/12 and C-594/12, ECLI:EU:C:2014:238) (CJEU Grand Chamber, Apr. 8, 2014), *Tele2 Sverige AB and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970) (CJEU Grand Chamber, Dec. 21, 2016); *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791) (CJEU Grand Chamber, Oct. 6, 2020.

394 *G.D. v. The Commissioner of the Garda Síochána and Others*, Case C-140/20, Court of Justice of the European Union, Grand Chamber, April 5, 2022 (ECLI:EU:C:2022:258). Another case, brought by German service providers, Joined Cases C-793/19 and C-794/19 (SpaceNet and Telekom Deutschland), is still pending at the CJEU, *see*, https://curia.europa.eu/juris/documents.jsf?num=C-793/19 (last access Aug. 20, 2022).

395 Apple Transparency Report (Government Requests January – June 2021), data also include numbers from past years, available on Apple's website at: https://www.apple.com/legal/transparency/jp.html (last access Oct. 10, 2022).

396 Apple Transparency Report (Government Requests January – June 2021), similarly, data also include numbers from past years, available on Apple's website at: https://www.apple.com/legal/transparency/fr.html (last access Oct. 10, 2022).

requests came from law enforcement.[397] However, compliance to such data requests are likely to be voluntary because in Japan, a warrant issued by a court would be required for any compulsory means of data collection by the law enforcement.[398] Such request, as a voluntary investigation (*nini sōsa*, 任意捜査), is regulated by Article 197(2) of the Code of Criminal Procedure. Like other democracies, law enforcement in Japan faces increasing pressure to exercise more control of the cyberspace: explosion of online abuse cases (ネット中傷), data breach, and the since assassination of Shinzo Abe, online information on weapons, etc. On the other hand, a vibrant civil society is demanding more privacy protection. The Japanese courts have long embraced the notion of informational self-determination—the Continental definition of privacy,[399] and occasionally do not shy away from controversies.[400] Japan is deeply invested in the idea of privacy as a personal right based on human dignity (*jinkaku ken*, 人格権), which is a lot closer to its European counterparts than to the third-party doctrine in the United States.

V. CONCLUSION

Surveillance states are embedded in and dependent on surveillance capitalism. To the extent that there is no way to escape from the dependence on data collected, stored, and processed by private tech companies, the symbiotic model that America created in the telegraph era has now spread to the rest of the world, together with the internet and social media. The basic elements of this model are as follows: data collectors are private and separate entities that are distinct from the surveillance state; the surveillance state is dependent on the data collectors for certain data, thus forming a symbiotic relationship; doctrinal and statutory frameworks are developed to create the channel for access to data; and a

---

397 LINE Transparency Report, available on LINE's website at: https://linecorp.com/en/security/transparency/2021h2 (last access Oct. 10, 2022).

398 Japanese Ministry of Justice, Collection and Use of Personal Information by Japanese Public Authorities for Criminal Law Enforcement and National Security Purposes 1-2 (Sept. 14, 2018) (memorandum prepared by the Japanese Ministry of Justice for European Commission), available on Japanese Personal Information Protection Commission (PPC, 個人情報保護委員) website at: https://www.ppc.go.jp/files/pdf/letter_government_access.pdf (last access Oct. 10, 2022).

399 始澤真純 [Masumi Shizawa], 日本におけるプライバシー権と自己情報コントロール権の発展 [*The Development of Privacy Rights and Self-control of Personal Information in Japan*], 東洋大学大学院紀要 55 [TOYO UNIVERSITY GRADUATE SCHOOL BULLETIN] 23-44 (Mar. 2019).

400 For example, in 2017, five years after United States v. Jones, 565 U.S. 400 (2012), the Supreme Court of Japan ruled that police in Japan violated citizens' privacy rights in using a global positioning system (GPS) in tracking the location of the accused without a search warrant, *see*, 最高裁第一小法廷判決・民集 62 巻 3 号 665 頁（平成 20 年 3 月 6 日[Sup. Ct. Japan, 62 Minshu 665, Mar. 6, 2017]. Another case was the Twitter case by the Supreme Court of Japan in 2020, *see*, Dongsheng Zang, *Revolt Against the U.S. Hegemony: Judicial Divergence in Cyberspace*, 39 WIS. INT'L L.J. 1, 64-65 (2022).

constitutional rule is managed by the judiciary to regulate the outer limits of this symbiotic relationship. From this perspective, this Article demonstrates, the symbiotic model can be traced by the legal doctrine of subpoena deuces tecum, from its telegraph era as a power of the grand jury, to the telephone era as an administrative power, and then—through the SCA—to laying the foundation for the internet and social media era. Its steady and persistent expansion together with the rapid progression of technology is the best representation of the making of a surveillance state in America.

For the rest of the world, however, the model is as new as the internet and social media. The surveillance state surely existed before the internet. It was not the symbiotic relationship, however, when the British Post Office was owned and controlled by the Queen. Therefore, privatization of the telecommunication industry in Commonwealth countries, the European Union, and Japan ("CEJ") is a key part of the transition to this new model. Along with this transition in the telecommunication industry, the legal framework in regulating the industry and access to data in these countries also followed the American model. Dynamics between industry and the surveillance state changed too. As Western Union, AT&T, Apple, and Microsoft joined the legal fight for privacy throughout American history, tech firms in the rest of the world are now involved in litigation together with citizens and stakeholders. Therefore, the symbiotic model of surveillance states prevailed not only in America, but in America's major trading partners in the age of the internet and social media.

The transition in CEJ, however, shed some light on the "prototype" of this model—the United States. While the transition in CEJ was started in the 1980s and accelerated in the 1990s, the United States was committed to the legal framework set forth in the SCA. The transition in CEJ was partially led and pushed by constitutional recognition of privacy as a fundamental right, reflected most visibly in wiretapping rulings by the European Court of Human Rights, and then in data retention rulings by the Court of Justice of the European Union. In the United States, however, all the Supreme Court did in *Jones*, and *Carpenter*, was to recycle the reasoning of *Miller* and *Smith v. Maryland*. While courts in CEJ played crucial roles in redefining privacy, the United States Supreme Court acted scared of the internet and were reluctant to take on privacy cases. Therefore, hidden in the triumph of the symbiotic model of surveillance states, is a rotten core in the American "prototype," where the judiciary is giving in to the surveillance state itself.