

Title	Chapter 2-II : The symbiotic model : the Leviathan and the Behemoths in America
Sub Title	
Author	Zang, Dongsheng
Publisher	Keio University Global Research Institute
Publication year	2025
Jtitle	Monsterizing Platform Power and Law ; Volume 1. Platforms and States: How to Settle the Battle of Monsters ,p.81- 91
JaLC DOI	10.14991/KO11003002.00000001-0081
Abstract	
Notes	Chapter 2 : The battle for the rulers of digital space
Genre	Book
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=KO11003002-00000001-0081

慶應義塾大学学術情報リポジトリ(KOARA)に掲載されているコンテンツの著作権は、それぞれの著作者、学会または出版社/発行者に帰属し、その権利は著作権法によって保護されています。引用にあたっては、著作権法を遵守してご利用ください。

The copyrights of content available on the Keio Associated Repository of Academic resources (KOARA) belong to the respective authors, academic societies, or publishers/issuers, and these rights are protected by the Japanese Copyright Act. When quoting the content, please follow the Japanese copyright act.

Chapter 2 - II

THE SYMBIOTIC MODEL

: The Leviathan and the Behemoths in America

Dongsheng Zang*

The revelation by Edward Snowden in June 2013 of the massive surveillance programs in the United States is a reminder of a ubiquitous and mighty Leviathan that overshadows a democracy.¹ However, in modern surveillance states, the Leviathan does not act alone; it gets able and crucial assistance from the Behemoths—the powerful digital platforms and service providers who are private firms. This chapter argues that the United States led the world in building a cozy and collaborative relationship between the Leviathan and the Behemoths, where a central function of modern law is to regulate and mediate government *access* to data collected by private firms. I will call this the symbiotic model of surveillance states.² The symbiotic model does not deny the continued efforts on the part of the Leviathan to collect, store, process and use data by its own apparatus and for its own purposes. It claims rather that the Leviathan and the Behemoths both have an insatiable appetite for data; they thrive even more when they work together.

1 Surveillance Models in Context

In 1890, when Samuel Warren and Louis Brandeis published their seminal article on the right to privacy,³ they were primarily complaining about tabloid press and the instant camera, the new technology at the time.⁴ In other words, they were complaining about private actors.⁵ Half a century later, however, English

* **Dongsheng Zang:** Associate Professor of Law, University of Washington School of Law, zangd@uw.edu

1 Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books 2014); Barton Gellman, *Dark Mirror: Edward Snowden and the American Surveillance State* (Penguin 2020).

2 I examined the symbiotic model in three areas of law in detail elsewhere, see, Dongsheng Zang, ‘Telegram, Telephone and the Internet: Making of the Symbiotic Model of Surveillance States’ [2023] 40 *Ariz J Int’l & Comp L* 1.

3 Samuel Warren and Louis Brandeis, ‘The Right to Privacy’ [1890] 4 *Harv L Rev* 193.

4 For the historical context of Brandeis’ article, see, Jeffrey Rosen, *Louis D Brandeis: American Prophet* (Yale University Press 2016), 40-42; James H Barron, ‘Warren and Brandeis, “The Right to Privacy” [1890] 4 *Harv L Rev* 193: Demystifying a Landmark Citation’ [1979] 13 *Suffolk U L Rev* 875.

5 Privacy litigation in the United States after the 1890 Warren-Brandeis article up to the 1960s was largely framed in tort law terms, see, William L. Prosser, ‘Privacy’ [1960] 48 *Calif L Rev* 383. Privacy litigation in the nineteenth-century France was similar, see, Wenceslas J Wagner, ‘The Development of the Theory of the Right to Privacy in France’ [1971] 1971 *Wash U LQ* 45; Wenceslas J Wagner, ‘The Right to One’s Own Likeness in French Law’ [1970] 46 *Ind LJ* 1.

writer George Orwell's novel *1984* shifted the paradigm by targeting the public actor—the state, the “Big Brother.”⁶ This was not accidental. In 1946, three years before his novel was published, Orwell wrote: “Every line of serious works that I have written since 1936 has been written, directly or indirectly, *against* totalitarianism and *for* democratic socialism.”⁷ Like Orwell, Anthony Giddens, the English sociologist, also saw a close connection between surveillance and totalitarianism: “Totalitarianism is, first of all, an extreme focusing of surveillance.”⁸ By contrast, French philosopher Michel Foucault's notion of surveillance (“panopticism”) is broader.⁹ Foucault did not specifically target the state apparatus; his theory of discipline as an instrument of power and domination went way beyond the state. However, there is still a close connection between the state and society. The clearest evidence is the question Foucault asked at the end of his chapter ‘Panopticism’: “Is it surprising that prisons resemble factories, schools, barracks, hospitals, which all resemble prisons?”¹⁰

What distinguishes classical writers such as Orwell, Giddens, and Foucault from contemporary commentators is that, when they were writing on surveillance, they were surrounded by *government data*—civil registration, passports, national identification cards, even telegrams, and telephone communications.¹¹ For a long time in European history, the telegraph and telephone industry was a state monopoly;¹² it was not privatized until the 1990s.¹³ Japan was similar. In September 1872, the Meiji government decided that no private telegraphs should be permitted. In May 1885, the Telegraph Code declared telegraphs a monopoly of the government.¹⁴ Nippon Telegraph and Telephone Company (NTT) remained a state-owned business until in July 1999, when it finally concluded its privatization process.¹⁵ Unlike Europe and Japan, however, the telecommunications industry was private business in the United States; thus the need to balance the state and the industry was felt long before the internet age.

6 George Orwell, *1984* (Secker & Warburg 1949).

7 George Orwell, ‘Why I Write’ (1946), in George Packer (ed), *Facing Unpleasant Facts: Narrative Essays* (Mariner Books 2008) 224-31, at 229 (emphasis in original).

8 Anthony Giddens, *The Nation-State and Violence* (University of California Press 1985) 303.

9 Michel Foucault, *Discipline and Punish: The Birth of the Prison* (Alan Sheridan trans 1977, 1975), 195-228.

10 *ibid* 228.

11 John Torpey, *The Invention of the Passport: Surveillance, Citizenship, and the State* (Cambridge 2000). Professor Daniel J. Solove considered the Big Brother model “fails to capture the most important dimension of the database problem.” Daniel J Solove, ‘Privacy and Power: Computer Databases and Metaphors for Information Privacy’ [2001] 53 *Stan L Rev* 1393, 1399.

12 Mila Davids, ‘The Relationship Between the State Enterprise for Postal, Telegraph and Telephone Services and the State in the Netherlands in Historical Perspective’ (1995) 24 [1] *Bus. & Econ. Hist.* 194, 196; Jean-Michel Johnston, *Networks of Modernity: Germany in the Age of the Telegraph, 1830-1880* (Oxford 2021). In Great Britain, telegraph was started by private entrepreneurs in 1838, but was brought to state ownership and control by the British Post Office in 1870, *see*, Hugo Richard Meyer, *The British State Telegraphs: A Study of the Problem of a Large Body of Civil Servants in a Democracy* (The Macmillan Company 1907) 75; Simone Fari, *Victorian Telegraphy Before Nationalization* (Palgrave Macmillan 2015).

13 Johan From and Kjell A Eliassen, *The Privatization of European Telecommunications* (Routledge 2007).

14 J Morris, ‘Telegraphs in Japan’ [1881] 10 *J of the Soc’y of Telegraph Engineers and of Electricians*; Shinjiro Mayeda, *Outlines of the History of Telegraphs in Japan* (1892) 27.

15 Marie Anchordoguy, ‘Nippon Telegraph and Telephone Company (NTT) and the Building of a Telecommunications Industry in Japan’ [2001] 75 *Bus Hist Rev* 507, 531.

2 The Behemoths in America

In America, the telegraph and telephone industry were led by such corporate giants as Western Union and AT&T—the Behemoths. Between the 1870s and 1980s, Western Union and AT&T fought the Leviathan in court over the interpretation of the Fourth Amendment of the United States Constitution, which prohibits unreasonable search and seizures.¹⁶ It is important to note that the Behemoths were not directly fighting for the privacy rights of their customers—they are not allowed to do that even if they wanted to. The United States Supreme Court held that “[t]he Fourth Amendment rights are personal rights which ... may not be vicariously asserted.”¹⁷ They were fighting for their own interests that happened to coincide with privacy rights of their customers.

(1) Western Union

Western Union Telegraph Company was founded in New York in 1851,¹⁸ and experienced phenomenal growth over the following years. By 1871, Western Union owned more than two-thirds of the telegraph wire and transmitted 90 percent of all the messages.¹⁹ Like the tech giants today, Western Union portrayed itself as an agent of peace and universal communication.²⁰ However, Western Union was troubled by frequent requests from the government for access to telegrams and fought in court to stop it. The first such case was *United States v. Babcock*.²¹ In January 1876, William Orton, president of the Western Union, was served a subpoena duces tecum—a legal instrument similar to *kōinjiō* (勾引状) in Japan—by the federal government in a criminal case to which the Western Union was not a party. The subpoena required Orton to produce telegrams. Western Union resisted the subpoena, but the court ruled to enforce it. The issue came up again in December 1876 when the United States House of Representatives issued a subpoena duces tecum on Edmund W. Barnes, manager of Western Union in New Orleans, Louisiana, to appear before a House special committee and produce “all telegrams” relating to an election fraud case.²² Barnes appeared in front of the committee but refused to produce the telegrams. Barnes was found in contempt by the House Judiciary

16 The Fourth Amendment provides:

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

The Fourth Amen., United States Constitution.

17 *Alderman v United States* 394 US 165, 174 (1969).

18 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* (Derby Brothers 1879) 464-67; Joshua D Wolff, *Western Union and the Creation of the American Corporate Order, 1845-1893* (Cambridge 2013).

19 Richard B du Boff, ‘The Telegraph in Nineteenth-Century America: Technology and Monopoly’ [1984] 26 *Comp Stud Soc & Hist* 571.

20 Richard R John, ‘Private Enterprise, Public Good?: Communications Deregulation as a National Political Issue, 1839–1851,’ in Jeffrey L Pasley, Andrew W Robertson and David Waldstreicher (eds), *Beyond the Founders: New Approaches to the Political History of the Early American Republic* (University of North Carolina Press 2004) 328-54.

21 *United States v Babcock* 24 FCas. 908 (CCED Mo 1876).

22 5 *Cong Rec* 352 (21 December 1876).

Committee.²³

A similar incident happened in St. Louis in April 1879,²⁴ 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, requiring him to testify before a grand jury and produce telegrams. Brown was found in contempt when he refused to produce the telegrams. Brown appealed, the case eventually went to the Supreme Court of Missouri.²⁵ While litigation was ongoing, Western Union mobilized its resources outside the courtroom. Henry Hitchcock, Western Union's lawyer, read his paper entitled "The Inviolability of Telegrams" at the Annual Meeting of the American Bar Association in August 1879.²⁶ 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.²⁷ Little was accomplished through these efforts. The Missouri Supreme Court declared that "[t]elegraphic messages are not privileged communications."²⁸

(2) AT&T

The telephone was invented in 1876.²⁹ By the mid-1880s, telephones had become widely used in New York.³⁰ In 1885, American Telephone and Telegraph Company (AT&T) was incorporated.³¹ In subsequent years, AT&T became the largest player in telecommunication until its breakup in 1984. In 1895, New York City began tapping telephones to collect evidence in criminal investigations.³² Wiretapping became widespread. In *Olmstead v. United States* (1928),³³ the United States Supreme Court was asked to decide whether evidence obtained by wiretapping without a warrant violated the Fourth Amendment. Major telephone companies including AT&T submitted *amici curiae* briefs against wiretapping.³⁴ They did not find a sympathetic ear in the Supreme Court.

In the 1970s, governments increasingly used administrative subpoena to access data held by third parties, including banks and telephone companies.³⁵ In *Reporters Committee for Freedom of Press v. AT&T* (1978),³⁶ journalists and newspapers filed a class action suit against AT&T, asserting that the Fourth Amendment requires *prior* notice before AT&T turned over their toll-billing records to law enforcement. AT&T adopted a

23 5 Cong Rec 602 (12 January 1877).

24 *Ex parte Brown* 7 Mo App 484 (St Louis Court of Appeal 1879).

25 *Ex parte Brown* 72 Mo 83 (1880).

26 Henry Hitchcock, 'The Inviolability of Telegrams' [1879] 5 South L Rev 473.

27 US 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).

28 *Ex parte Brown* 72 Mo. 83, at 90 (1880).

29 Alvin Fay Harlow, *Old Wires and New Waves: The History of the Telegraph, Telephone, and Wireless* (D. Appleton-Century Company 1936) 356-60.

30 *ibid* 394.

31 *ibid* 398; NR Danielian, *AT&T: The Story of Industrial Conquest* (Vantage Books 1939) 12.

32 Brian Hochman, *The Listeners: A History of Wiretapping in the United States* (Harvard University Press 2022) 59.

33 *Olmstead v United States* 277 US 438 (1928).

34 This included the Pacific Telephone and Telegraph Company, American Telephone and Telegraph Company (AT&T), United State Independent Telephone Association, and the Tri-State Telephone and Telegraph Company, *ibid* at 452.

35 Donald RC Pongrace, 'Requirement of Notice of Third-Party Subpoenas Issued in SEC Investigations: A New Limitation on the Administrative Subpoena Power' [1984] 33 Am U L Rev 701 (Comment).

36 *Reporters Committee for Freedom of Press v AT&T* 593 F2d 1030 (DC Cir 1978), *cert. denied*, 440 US 949 (1979).

notification policy in March 1974, which only undertook notification *after* subpoena.³⁷ Plaintiffs considered the policy inadequate. The United States federal government intervened as a party defendant. The Federal Court of Appeals for the D.C. Circuit ruled in favor of AT&T and the United States. A central justification for the ruling was that the toll record was the telephone company's property; therefore when government inspected the toll record, there was no violation of the Fourth Amendment.³⁸

What the D.C. Circuit Court used was the prevailing view of the Fourth Amendment, known as the third-party doctrine, articulated by the Supreme Court in *United States v. Miller* (1976),³⁹ and then in *Smith v. Maryland* (1979).⁴⁰ In *Miller*, a tax fraud case, police obtained records from suspect's banks without a warrant. The suspect contended that bank records were his "private papers." The Court rejected the argument, stating that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."⁴¹ In *Smith*, police, without a warrant, installed a pen register at the telephone company's central office in order to record the numbers dialed from the telephone at suspect's home. The Court rejected that claim stating, "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."⁴² The third party doctrine in *Miller* and *Smith* became an effective tool to enable the government to access data held by private companies. It is the central element of the symbiotic model of surveillance states.

3 Legal Framework of the Symbiotic Model

From the 1970s, the legal framework for a symbiotic relationship between the private telecommunications industry and the U.S. government was formed. This includes the following three elements: (1) a narrow interpretation of the Fourth Amendment based on the third-party doctrine; (2) a statutory framework that enabled government access to data held by the telecommunications service providers; and (3) a broad immunity provided by statute to the service providers.

(1) The Fourth Amendment

The third-party doctrine, though debated,⁴³ was extended to the cyberspace through the Supreme Court

37 *ibid* 1038.

38 *ibid* 1045 (emphasis added).

39 *United States v. Miller*, 425 US 435 (1976).

40 *Smith v. Maryland*, 442 US 735 (1979).

41 *Miller* (n 39) 443.

42 *Smith* (n 40) 743-44.

43 Orin S Kerr, 'The Case for the Third-Party Doctrine' [2009] 107 Mich L Rev 561; Orin S Kerr, 'Defending the Third-Party Doctrine: A Response to Epstein and Murphy' [2009] 24 Berkeley Tech LJ 1229; Erin Murphy, 'The Case against the Case for Third-Party Doctrine: A Response to Epstein and Kerr' [2009] 24 Berkeley Tech LJ 1239.

ruling in *United States v. Carpenter* (2018).⁴⁴ In this case, after a series of robberies in Detroit, the police sought, by a court order, and obtained cell-site location information (CSLI) of Timothy Carpenter from two wireless carriers without a warrant. After he was convicted, Carpenter moved to suppress the CSLI evidence based on the Fourth Amendment. A central issue was whether Carpenter had a reasonable expectation of privacy in CSLI. Following the third-party doctrine, the police argued that he did not have a reasonable expectation of privacy because he shared the CSLI with his cell phone companies, and those data were business records of the phone companies. The majority of the Court disagreed with the government position, not because they rejected the third-party doctrine, but on the question of how far the third-party doctrine should go:

We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection.⁴⁵

The Court considered location data to be an “entirely different species of business record.”⁴⁶ Trying to grasp the nuance of the modern technology, the Court reasoned: wireless carriers “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.”⁴⁷

Privacy advocates won the battle but lost the war.⁴⁸ The victory was a narrow one—it is only on historical CSLI, not even on real time cell site location data, or other data.⁴⁹ The Court insisted that “[w]e do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information.”⁵⁰ In other words, the *Carpenter* majority brought the third-party doctrine to the digital age and solidified the principle that AT&T had fought in the 1970s without success.

(2) Statutes on Government Access to Data

In *Carpenter*, the police relied on a court order according to 18 U.S.C. § 2703(d), part of a federal statute

⁴⁴ *United States v. Carpenter* 585 US 296, 138 SCt 2206 (2018).

⁴⁵ 138 SCt 2206, 2217.

⁴⁶ *ibid* 2222.

⁴⁷ *ibid* 2219.

⁴⁸ Alan Z Rozenstein, ‘Fourth Amendment Reasonableness after *Carpenter*’ [2019] 128 Yale LJ F 943, 952 (arguing “that the third-party doctrine, ... is hopelessly flawed and should be broadly cut back, if not abandoned entirely.”). More commentators, however, welcomed and praised the *Carpenter* ruling, *see*, Paul Ohm, ‘The Many Revolutions of *Carpenter*’ [2019] 32 Harv J L & Tech 357; Susan Freiwald & Stephen Wm Smith, ‘The *Carpenter* Chronicle: A near-Perfect Surveillance’ [2018] 132 Harv L Rev 205.

⁴⁹ *Carpenter* (n 44) 2220 (“Our decision today is a narrow one. 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)”).

⁵⁰ *ibid* 2220.

known as the Stored Communication Act (“SCA”).⁵¹ By comparison, a warrant requires “probable cause,” a higher standard compared to that for a court order.⁵² SCA was enacted in 1986 as Title II of the Electronic Communications Privacy Act of 1986 (“ECPA”).⁵³ The 1986 ECPA reflected the grand bargaining in the 1980s between the Department of Justice on the one hand, and the telecommunications industry and privacy groups on the other.⁵⁴ This was adjacent to the time that AT&T was breaking up in 1984, and new technologies such as cellular phone services and email became significant. SCA diluted the Fourth Amendment warrant requirement by creating a framework for law enforcement to have access to contents of communication and subscriber data by different legal instruments under Sec. 2703.⁵⁵ Access to contents of communication that had been recorded within the past 180 days had the most strict rule: a warrant.⁵⁶ For access to non-content data, Sec. 2703(c) provided the maximum flexibility to law enforcement: either a warrant, administrative subpoena, grand jury subpoena, or a court order would be adequate.⁵⁷ Over time, with the rise of the internet, social media and datamining, non-content data became increasingly essential in revealing user’s privacy. However, the government’s power to access data under Sec. 2703 only became stronger by a series of federal statutes.

The first such move was the Communications Assistance for Law Enforcement Act (“CALEA”) of 1994.⁵⁸ CALEA requires telecommunication carriers to ensure that they have the capacity to enable the government to intercept all wire and electronic communications.⁵⁹ It also amended Sec. 2703(c) by allowing the gov-

51 Stored Communication Act (“SCA”), 18 USC § 2701 et seq.

52 *Carpenter* (n 44) 2221 (noting that “a court order issued under the Stored Communications Act, which required the Government to show ‘reasonable grounds’ for believing that the records were ‘relevant and material to an ongoing investigation.’ 18 USC § 2703(d). That showing falls well short of the probable cause required for a warrant.”).

53 Electronic Communications Privacy Act (“ECPA”) of 1986, PL 99-508 (21 October 1986) 100 Stat 1848.

54 For the legislative history of ECPA, see, S Rep No 99-541 (1986); Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press 1995) 109-43 (on the legislative process of ECPA); Orin S Kerr, ‘A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It’ [2004] 72 Geo Wash L Rev 1208; Deirdre K Mulligan, ‘Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act’ [2004] 72 Geo Wash L Rev 1557. The first federal statute giving police the power to intercept telecommunications was the Omnibus Crime Control and Safe Streets Act of 1968, PL 90-351, 82 Stat 197 (19 June 1968), codified at 34 USC § 10101 et seq. (2020). The 1968 Act outlawed wiretapping by private parties, § 802, 82 Stat 213, and required a search warrant issued by a federal judge for authorized wiretapping, § 802, 82 Stat 216. ECPA gave police more power by relaxing the warrant requirement.

55 Sec. 201, ECPA (n 53) 100 Stat 1860. The observation of Oren Bar-Gill and Barry Friedman sounds true in the case of SCA, see, Oren Bar-Gill and Barry Friedman, ‘Taking Warrants Seriously’ [2012] 106 Nw U L Rev 1609, 1620 (“In theory, the rule is that police must obtain warrants before searching, but in reality, the exceptions to the warrant requirement have eaten up the rule.”). Note, however, the other school of thought does not read the Fourth Amendment as a “warrant requirement,” see, Akhil Reed Amar, ‘Fourth Amendment First Principles’ [1994] 107 Harv L Rev 757, 759 (“We need to read the Amendment’s words and take them seriously: they do not require warrants, probable cause, or exclusion of evidence, but they do require that all searches and seizures be reasonable.”).

56 Sec 201, ECPA (n 53) 100 Stat 1861, codified as §2703(a).

57 Sec 201, ECPA (n 53) 100 Stat 1862, codified as §2703(c)(1)(B).

58 Communications Assistance for Law Enforcement Act (“CALEA”) of 1994, PL. No. 103-414, (25 October 1994) 108 Stat. 4279, codified at 47 U.S.C. §§ 1001-10 (2020). For the legislative history, see, Susan Freiwald, ‘Uncertain Privacy: Communication Attributes after the Digital Telephony Act’ [1996] 69 S Cal L Rev 949; Lillian R BeVier, ‘The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break Up of AT&T’ [1999] 51 Stan L Rev 1049.

59 Sec 103, CALEA, codified as 47 USCA § 1002 (1998). Professor Lillian R BeVier commented, “CALEA is not simply the next installment of a technologically impelled statutory evolution. Instead, in terms of the nature and magnitude of the interests it purports to ‘compromise’ and the industry it seeks to regulate, in terms of the extent to which it purports to coerce private sector solutions to public sector problems, and in terms of the foothold it gives government to control the design of telecommunications networks, the Act is a paradigm shift.” BeVier (n 58) 1102-03.

ernment to use administrative subpoena or grand jury subpoena to access subscriber information including name, address, telephone toll billing records, etc.⁶⁰ The second major move was the USA Patriot Act of 2001,⁶¹ which expanded voluntary disclosure under Sec. 2702,⁶² and required disclosure under Sec. 2703.⁶³ In 2015, the USA Freedom Act was passed during the Obama administration,⁶⁴ but its reform was more on foreign intelligence, not on domestic law enforcement access to data.

(3) Communication Decency Act 1996

Section 230 of the Communication Decency Act (“CDA”) was initially enacted in 1996 as part of Title V of the Telecommunications Act.⁶⁵ When the CDA was proposed in 1995, Senator James Exon was primarily concerned about online pornography.⁶⁶ In June 1997, however, the United States Supreme Court struck down parts of the Act for abridging freedom of speech under the First Amendment.⁶⁷ As a result, Sec. 230 became 230(c)(1): “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”⁶⁸ Over time, Sec. 230 was interpreted by courts as a general immunity for internet service providers from civil liabilities.⁶⁹

While Sec. 230 has been questioned widely, it remains intact. In *Force v. Facebook* (2019),⁷⁰ American victims of terrorist attacks by Hamas in Israel contended that digital platforms like Facebook should be held accountable for the algorithms designed to recommend content related to terrorism. The Federal Court of Appeals for the Second Circuit rejected the claims, and relying on Sec. 230, stated:

Merely arranging and displaying others’ content to users of Facebook through such algorithms... is not enough to hold Facebook responsible as the “develop[er]” or “creat[or]” of that content.⁷¹

Two years later, a similar question was brought to the Federal Court of Appeals for the Ninth Circuit in *Gonzalez v. Google* (2021).⁷² The Ninth Circuit shared the view of the Second Circuit in *Force* and ruled in

⁶⁰ Sec 207, CALEA, 108 Stat 4292, codified as 18 USCA § 2703(c)(2) (2019).

⁶¹ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (“USA Patriot Act”) of 2001, PL. No 107-56, 115 Stat 272 (October 26, 2001).

⁶² Sec 212, USA Patriot Act, 115 Stat 284.

⁶³ Sec 212, USA Patriot Act, 115 Stat 285.

⁶⁴ Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015 (“USA Freedom Act”), PL No 114-23, 129 Stat 268 (2 June 2015).

⁶⁵ Telecommunications Act of 1996, PL 104-104, § 230, 110 Stat 56, 137-39.

⁶⁶ Robert Cannon, ‘The Legislative History of Senator Exon’s Communications Decency Act: Regulating Barbarians on the Information Superhighway’ [1996] 49 Fed Commc’ns LJ 51, 53; Vikas Arora, ‘The Communications Decency Act: Congressional Repudiation of the “Right Stuff”’ [1997] 34 Harv J on Legis 473, 474 (Note).

⁶⁷ *Reno v ACLU*, 521 US 844, 849 (1997).

⁶⁸ 47 USC § 230(c)(1).

⁶⁹ Dongsheng Zang, ‘Revolt against the U.S. Hegemony: Judicial Divergence in Cyberspace’ [2021] 39 Wisconsin Int’l L . 1, 43-56 (examining negligence standards for service providers in the laws of British Commonwealth countries, the European Union, Japan and China).

⁷⁰ *Force v Facebook Inc*, 934 F.3d 53, 74 (2nd Cir 2019).

⁷¹ *ibid* 70.

⁷² *Gonzalez v Google*, 2 F4th 871, 888 (9th Cir 2021), *vacated on other grounds*, *Gonzalez v Google*, 598 US 617 (2023), *Twitter v Taamneh*, 598 US 471 (2023).

favor of Google. The case was eventually brought to the Supreme Court, but the Supreme Court vacated the Ninth Circuit's ruling on other grounds, leaving the question of Sec. 230 unanswered.⁷³

4 The Behemoths in the Social Media Age

After the September 11 attacks, telecommunications and internet service providers found themselves under more pressure to collaborate with the government.⁷⁴ Some years later we learned that AT&T was a eager partner to the National Security Agency by voluntarily transferring vast amounts of telephone and internet information of their customers.⁷⁵ In the age of social media, the Behemoths continue fighting the Leviathan, though the symbiotic model is more entrenched and thus there is much less room to negotiate.

In *Carpenter* litigation, tech companies including Airbnb, Apple, Box, Cisco Systems, Dropbox, Facebook, Google, Microsoft, Snap, Twitter, and Verizon filed their joint *amici curae* brief, urging that “Fourth Amendment protections for digital data should be strong.”⁷⁶ In particular, the tech companies specifically argued that the third-party doctrine “make[s] little sense in the context of digital technologies and should yield to a more nuanced understanding of reasonable expectations of privacy.”⁷⁷

Within the framework of SCA, the tech companies continued pushing the envelope. In March 2010, a broad array of civil liberties groups, think tanks and tech companies formed a Digital Due Process coalition,⁷⁸ tasked to press Congress to reform SCA. In particular, they wanted Congress to require a search warrant for the government to access data held by service providers.⁷⁹ The effort did not go very far. In the *Microsoft Email* case,⁸⁰ Microsoft challenged a warrant issued under Sec. 2703, on the ground that the warrant did not reach data stored outside the U.S. territory. The Second Circuit agreed.⁸¹ However, Congress

73 Adam Liptak, ‘Supreme Court Delivers 2 Wins to Tech Giants: Legal Shield for Users’ Posts Holds, for Now’ *NY Times*, (19 May 2023) A1.

74 Albert Gidari Jr, ‘Companies Caught in the Middle’ [2007] 41 *USF L Rev* 535, 541 (“The government no longer is patient with service providers who delay, argue, review process, complain about it, or push back.”). See also David Lyon, *Surveillance After September 11* (Wiley 2003); Charles H Kennedy and Peter P Swire, ‘State Wiretaps and Electronic Surveillance after September 11’ [2002-2003] 54 *Hastings LJ* 971.

75 It was first revealed in May 2006 by the *New York Times*, subscribers then filed lawsuits against AT&T, see, *Hepting v AT&T*, 439 FSupp2d 974 (ND Calif 2006) remanded by the Ninth Circuit on appeal, *Hepting v AT&T*, 539 F3d 1157 (9th Cir 2008); *In re National Security Agency Telecommunications*, 671 F3d 881 (9th Cir 2011) cert. denied, *Hepting v AT&T*, 568 US 958 (2012). Jon D Michaels, ‘All the President’s Spies: Private–Public Intelligence Partnerships in the War on Terror’ [2008] 96 *Calif L Rev* 901, 912.

76 Brief for Technology Companies as *Amici Curiae* in Support of Neither Party (No 16-402), Aug. 14, 2017, 2017 WL 3530959 (US) (Appellate Brief).

77 *ibid* 1-2.

78 Miguel Helft, ‘A Wide Call To Improve Web Privacy’ *NY Times*, (31 March 2010) B1.

79 ‘Our Principles’ *Digital Due Process* <<https://digitaldueprocess.org/our-principles/>> accessed 1 November 2023. For comments on its proposals, Orin S Kerr, ‘The Next Generation Communications Privacy Act’ [2014] 162 *U Pa L Rev* 373, 386–90.

80 *In the matter of a Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation* 829 F3d 197 (2nd Cir 2016) vacated and remanded by the Supreme Court in *United States v Microsoft* 585 US ___, 138 S.Ct. 1186 (2018).

81 The Second Circuit ruling was based on a statutory interpretation cannon “presumption against extraterritoriality.” However, a federal district court in Pennsylvania reached a different conclusion in a similar case, *In re Search Warrant No 16-960-M-01 To Google*, 232 FSupp3d 708 (ED Pa 2017). See, Paul M Schwartz, ‘Legal Access to the Global Cloud’ [2018] 118 *Colum L Rev* 1681.

clarified the issue by enacting the CLOUD Act,⁸² making it explicit that disclosure of subscriber 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”⁸³ is required.

In a divided America, controversies of the content moderation intensified in recent years—on election fraud, COVID-19 lab-leak theory, vaccine side-effects, the Hunter Biden laptop story, etc. In May 2020, President Trump issued an Executive Order targeting “online censorship.”⁸⁴ Challenges to the Executive Order were dismissed.⁸⁵ In July 2021, Florida passed a law prohibiting large social media platforms from de-platforming candidates for office;⁸⁶ similarly, in September 2021, Texas passed a law prohibiting social media platforms from censoring users based on their viewpoints.⁸⁷ Both laws are being challenged in court, the Supreme Court, however, has not given a clear answer. Other measures are more subtle. Does a civil investigation on a digital platform constitute a violation of the First Amendment?⁸⁸ What about letting the Secretary of State flag tweets on Twitter?⁸⁹ Does the pressure from the White House on “misinformation” constitute violation of the First Amendment?⁹⁰ These are crucial questions that the answers to from the Supreme Court will shape the balance of power between the Leviathan and the Behemoths in the near future.

5 Conclusion

Among classical surveillance writers, Anthony Giddens did not consider surveillance unique to totalitarian states. Writing in the early 1980s, Giddens was sensitive to the fact that surveillance was needed

82 The Clarifying Lawful Overseas Use of Data Act or CLOUD Act (HR 4943), Division V of the Consolidated Appropriations Act, 2018, PL 115-141, 132 Stat 348 (23 March 2018).

83 Sec 103, CLOUD Act, 132 Stat 1213–14, codified as 18 U.S.C. § 2713. Tim Cochrane, ‘Hiding in the Eye of the Storm Cloud: How Cloud Act Agreements Expand U.S. Extraterritorial Investigatory Powers’ [2021] 32 Duke J Comp & Intl L 153.

84 Executive Order No 13,925, 85 Fed Reg 34,079 (28 May 2020).

85 Two cases were brought to the courts. One was *Rock the Vote v Trump*, No 20-cv-06021-WHO 2020 WL 6342927 (ND Calif 29 Oct. 2020). The other was *Center for Democracy & Technology v Trump*, 507 FSupp3d 213 (DDC 2020) *appeal dismissed as moot* by the Court of Appeals for the District of Columbia Circuit, *Center for Democracy & Technology v Trump*, No. 21-5062 2021 WL 11659822 (DCC 9 August 2021). In both cases, plaintiffs’ motion for a preliminary injunction was denied for failure to establish “injury in fact” in order to satisfy Article III standing.

86 Florida Senate Bill 7072, adopted by the Florida Legislature (1 July 2021) Chapter No 2021-32 *available at* <<https://www.flsenate.gov/Session/Bill/2021/7072/>> accessed 1 November 2023. *NetChoice LLC v Attorney General Florida*, 34 F4th 1196 (11th Cir 2022) (affirming lower court’s granting of preliminary injunction), *vacated and remanded*, *Moody v NetChoice*, 144 SCt 2383 (2024).

87 On September 9, 2021, Texas Governor Gregory Wayne Abbott signed into law House Bill 20, *available at* <<https://capitol.texas.gov/BillLookup/Text.aspx?LegSess=872&Bill=HB20>> accessed 1 November 2023. *NetChoice LLC v Paxton* 49 F4th 439 (5th Cir 2022) (vacating lower court’s granting of preliminary injunction and remanding the case back to federal district court in Western District of Texas), *vacated and remanded*, *Moody v NetChoice* 144 SCt 2383 (2024).

88 *Twitter Inc. v Paxton* 56 F4th 1170 (9th Cir 2022) (dismissing Twitter’s allegation that Texas Attorney General’s civil investigative demand constituted a violation of operator’s Freedom of Speech rights).

89 *O’Handley v Weber* 62 F4th 1145 (9th Cir 2023) (affirming lower court’s dismissal of a political commentator’s complaint against Twitter and California Secretary of State alleging collaborative relationship between the two).

90 *Missouri v Biden* 83 F4th 350 (5th Cir 2023) (finding that the White House, acting in concert with the Surgeon General’s office, likely coerced the platforms to make their moderation decisions by way of intimidating messages and threats of adverse consequences, and significantly encouraged the platforms’ decisions by commandeering their decision-making processes, both in violation of the First Amendment), *reversed and remanded*, *Murphy v Missouri*, 144 S.Ct. 1972 (2024).

for welfare distribution in democratic states too.⁹¹ Giddens might have sensed that surveillance could even function as a vehicle through which a democracy transforms itself into a totalitarian state when he warned: “Totalitarianism, I shall claim, is a tendential property of the modern state.”⁹² Giddens did not explain how. He did not anticipate that soon after his book was published in 1985, the Stored Communication Act of 1986, which laid the foundation for a symbiotic model of surveillance state, provided the answer.

91 Giddens (n 8) 309.

92 *ibid* 295. In 1979, the English High Court ruled that wiretapping by police without warrant was not a violation of English law, *see, Malone v Metropolitan Police Commissioner (No 2)*, [1979] EWHC 2 (Ch), [1979] Ch. 344, [1979] 2 All ER 620. The European Court of Human Rights found violation of the European Convention, *Malone v the United Kingdom*, Judgment (Merits), App No 8691/79 (A/82), [1984] ECHR 10.