ADAPTING *BARTNICKI V. VOPPER* TO A CHANGING TECH LANDSCAPE: REBALANCING FREE SPEECH AND PRIVACY IN THE SMARTPHONE AGE

Andrew E. Levitt*

> [A] principle, to be vital, must be capable of wider application than the mischief which gave it birth. This is peculiarly true of constitutions.
>
> —Weems v. United States[1]

---

* Student, William & Mary Law School Class of 2019. Many thanks to the *William & Mary Bill of Rights Journal* editorial staff, and to Professor Paul Marcus, who may or may not remember talking me out of an extremely far-fetched Note topic.

[1] 217 U.S. 349, 373 (1910).

INTRODUCTION

Every day in 2018, enough bytes cross the internet to encode 200,000 years of DVD-quality video.[2] By 2021, data volume is expected to roughly double.[3] Not only are data moving in supermassive quantities, servers are quietly sweeping a wider variety of data from a startling range of interconnected devices and apps.[4] Web-connected products from televisions to fitness bracelets to thermostats leave an online data trail,[5] potentially vulnerable to inspection, misuse, and theft.[6]

Federal and state governments have a range of tools to protect Americans' personal data from such intrusions. Various hacking activities, wiretapping, "spoofing," identity theft, and certain misrepresentations are already illegal.[7] But one scenario is relatively shielded from sanction: if a hacker launders stolen data to a third party, the third party often has the blessing of the First Amendment to publish it.

To understand this story, I begin with Title III of the Crime Control and Safe Streets Act of 1968, also called the Wiretap Act. The Wiretap Act, as currently amended, prohibits various invasions and disclosures of wire, oral, and electronic communications.[8] Among other things, the Act authorizes both criminal and civil causes of action for private hacking and wiretapping activities,[9] prohibits unauthorized sharing of an authorized law enforcement wiretap,[10] and prohibits the *use* of stolen information, such as for commercial purposes.[11] Section 2511(1)(c), however, deals not with the commission of a wiretapping offense, but with disclosure: it prohibits disclosure of information when the disclosing party knew or should have known the communications were obtained by unlawful interception.[12] In § 2511(1)(c), Congress deemed

---

[2] *See The Zettabyte Era: Trends and Analysis*, CISCO (June 7, 2017), https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html [https://perma.cc/HZ5E-GZC9] (giving overview of trends in communications and network technology); 2 TONY PEARSON, INSIDE SYSTEM STORAGE 95 (2010).

[3] *See* CISCO, *supra* note 2.

[4] *See* PEARSON, *supra* note 2.

[5] *See* CISCO, *supra* note 2.

[6] *See id.*

[7] *See* 18 U.S.C. § 2511(1)(a)–(b) (2012).

[8] *See* Pub. L. No. 90-351, §§ 2511–2520, 82 Stat. 197, 213–25 (1968) (codified as currently amended at 18 U.S.C. §§ 2510–20 (2012)).

[9] 18 U.S.C. § 2511(1)(d); § 2520(a).

[10] § 2511(1)(e). The elements of § 2511(1)(e) essentially require a knowing obstruction of a law enforcement investigation. *See id.*

[11] *See* § 2511(1)(d).

[12] The Wiretap Act of 1968 was amended in 1986 to include electronic data interceptions and thefts, in addition to wiretapping. *See* Elec. Comms. Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986); *see also* the statutory text, *infra* note 26. Accordingly, in this Note, the terms "wiretap" or "wiretapping" should be generally understood, unless otherwise implied, to include interception of any wire, oral, or electronic communication.

the publication of one's stolen private communications sufficiently subversive of "the comforts of society" as to merit the recourse of the law.[13] Lawmakers sought to protect private speech and to deter the amplification of stolen conversations.[14] Most states adopted similar statutes.[15]

Under the federal statute, the disclosing party may be the wiretapper herself *or another*.[16] The disclosing party might be innocent in the initial theft, but liable for spreading the fruits of such theft.[17] The third-party publisher in the three-party scenario has herself invaded no private communications; she is (in theory) merely sharing what she has found. What are the legitimate Free Speech interests of the publisher?

In 2001, the First Amendment met such an application of § 2511(1)(c) of the Wiretap Act head-on in *Bartnicki v. Vopper*.[18] In *Bartnicki*, the Supreme Court addressed

---

[13] Entick v. Carrington, 19 Howell's St. Trials 1029, 1066 (C.P. 1765).

[14] *See* 18 U.S.C. §§ 2511–2020.

[15] *See* ALA. CODE § 13A-11-35 (2018); ALASKA STAT. ANN. § 42.20.300(d) (West 2017); ARK. CODE ANN. § 5-60-120(c)(3) (West 2017); CAL. PENAL CODE § 631(a) (West 2018); COLO. REV. STAT. § 18-9-303(c) (2018); DEL. CODE ANN., tit. 11, § 1335(a)(5) (2018); D.C. CODE § 23-542(a)(2) (2018); FLA. STAT. §§ 934.03(1)(c)–(e) (2017); GA. CODE ANN. § 16-11-62(5) (2017); HAW. REV. STAT. § 803-42(a)(3) (2017); IDAHO CODE § 18-6702(1)(c) (2017); 720 ILL. COMP. STAT. 5/14-2(a)(5) (2018) (invalidated as overbroad in People v. Clark, 6 N.E.3d 154 (Ill. 2014); People v. Melongo, 6 N.E.3d 120 (Ill. 2014)); IOWA CODE § 808B.2(1)(c) (2017); KAN. STAT. ANN. § 21-6101(a)(2) (2017); KY. REV. STAT. ANN. § 526.060 (West 2018); LA. STAT. ANN. § 15:1303 (2017); ME. STAT. tit. 15, § 710(3) (2017); MD. CODE ANN., CTS. & JUD. PROC. § 10-402(a)(2) (West 2018); MASS. GEN. LAWS ch. 272, § 99(C)(3) (2017); MICH. COMP. LAWS §§ 750.539d & 750.539e (2018); MINN. STAT. § 626A.02(1)(3) (2017); MO. REV. STAT. § 542.402(1)(3) (2017); NEB. REV. STAT. § 86-290(1)(c) (2017); NEV. REV. STAT. § 200.630 (2017); N.H. REV. STAT. ANN. § 570-A:2(I)(c) (2018); N.J. REV. STAT. § 2A:156A-3(b) (2017); N.M. STAT. ANN. § 30-12-1 (2018); N.Y. PENAL LAW § 250.25(4) (McKinney 2018); N.C. GEN. STAT. § 15A-287(a)(3) (2017); N.D. CENT. CODE § 12.1-15-02(1)(b) (2017); OKLA. STAT., tit. 13, § 176.3(3) (2018); ORE. REV. STAT. § 165.540(1)(e) (2018); 18 PA. CONS. STAT. § 5703(2) (2018); 11 R.I. GEN. LAWS § 11-35-21(a)(2) (2017); S.C. CODE ANN. § 17-30-20(3) (2017); TENN. CODE ANN. § 39-13-601(a)(1)(C) (2017); TEX. PENAL CODE ANN. § 16.02(b)(2) (2017); UTAH CODE ANN. § 77-23a-4(1)(b)(iii) (2017); VA. CODE ANN. § 19.2-62(A)(3) (2018); W. VA. CODE § 62-1D-3(a)(2) (2017); WIS. STAT. § 968.31(1)(c) (2018); WYO. STAT. ANN. § 7-3-702(a)(iii) (2017); *see also* CONN. GEN. STAT. § 54-41p (2017); IND. CODE § 35-33.5-5-4(a) (2017); KAN. STAT. ANN. § 21-5923 (2017); MISS. CODE ANN. § 41-29-511 (2017); MONT. CODE ANN. § 45-8-213 (2017); OHIO REV. CODE ANN. § 2933.52(A) (2017); S.D. CODIFIED LAWS § 23A-35A-18 (2018); VT. STAT. ANN. tit. 13, § 8108 (2017); WASH. REV. CODE § 9.73.030 (2018); P.R. LAWS ANN. tit. 25, § 285q (2017).

[16] *See* 18 U.S.C. § 2511(1)(c).

[17] *See id.*

[18] 532 U.S. 514 (2001). For those interested, the petitioner's name is apparently pronounced as the Americanized "Bartnicky," and not the Polish "Bartnitzky." *See* Oral Argument at 0:07, 2:49, Bartnicki v. Vopper, 532 U.S. 514 (2001) (No. 99-1687), https://apps.oyez.org/player/#/rehnquist10/oral_argument_audio/22162 [https://perma.cc/KJD9-8UX4].

whether it is constitutional to punish the publication "[w]here the punished publisher of information has obtained the information in question in a manner lawful in itself but from a source who has obtained it unlawfully. . . ."[19] A fractured Court held that such communications—when truthful and regarding matters of "public concern"—are protected under the First Amendment.[20]

But "time works changes, brings into existence new conditions and purposes."[21] In the years since *Bartnicki*, the facts of which occurred in 1993,[22] communications technology has transformed. Petabytes of emails, photographs, texts, voicemails, and other documents now transmit through the web and are stored and maintained on the "cloud"—often without the understanding of the communicant.[23] High-profile incidents of hacking of private communications, including intimate personal information and photographs, have raised the issues of illegally sourced information and "public concern" to the fore.[24]

In this Note, I argue that vast technosocial changes arising since *Bartnicki* shift the constitutional balance of interests sufficiently such that *Bartnicki* should be abrogated. While the Free Speech interests at the heart of *Bartnicki* are no less important today than in 2001, the risks to private communicants are dramatically higher such that the Free Speech Clause must yield way. I propose that the *Bartnicki* doctrine should be tailored to allow legislators a wider range of lawful controls on the publication of stolen information.

In Part I of this Note, I discuss the contours of the holding, concurrence, and dissent in *Bartnicki*, the holding's implications, and how it has applied since 2001. In Part II, I discuss the expansion of information technology, information collection, and hacking and eavesdropping risks. These technosocial changes are so substantial that even reasonable communicants cannot protect all their private communications. I argue, therefore, that these overwhelming technosocial changes justify revisiting *Bartnicki*. In Part III, I argue that the Supreme Court often evaluates and reevaluates doctrine in response to technosocial changes, and that it is uncontroversial to suggest the Court should revisit a holding for this reason. Finally, in Part IV, I discuss the

---

[19] *Bartnicki*, 532 U.S. at 528 (quoting Boehner v. McDermott, 191 F.3d 463, 484–85 (D.C. Cir. 1999) (Sentelle, J., dissenting)).

[20] *Id.*

[21] Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

[22] *See Bartnicki*, 532 U.S. at 518.

[23] *See, e.g.*, Tim Fisher, *Terabytes, Gigabytes, and Petabytes: How Big Are They?*, LIFEWIRE (May 10, 2018), https://www.lifewire.com/terabytes-gigabytes-amp-petabytes-how-big-are-they-4125169 [https://perma.cc/US46-LCR8]; Bureau International Des Poids et Mesures, *Resolution 10 of the 15th CGPM* (1975), https://www.bipm.org/en/CGPM/db/15/10/ [https://perma.cc/N364-GHWR] (adopting "peta" as the Système International prefix for the multiplying factor of 10^15).

[24] *See infra* Section II.B; *see also infra* notes 230–34 and accompanying text.

difficult balance of privacy, free speech, and free press interests, and propose ways the Court should loosen the doctrine to allow legislatures to deter publication of the fruits of illegal snooping activity. I argue that in the *Bartnicki* context, Fourth Amendment principles converge with the First Amendment, and the Court should borrow certain concepts of reasonable expectation of privacy and control.

I. THE PRINCIPAL CASE: *BARTNICKI V. VOPPER*

The Wiretap Act established new laws regarding the interception and dissemination of private oral and wire communications.[25] Among other things, the Wiretap Act prohibited disclosure of information when the disclosing party knew or should have known that the communications were obtained unlawfully.[26] The purpose of the law, set forth in the committee report, was to "protec[t] the privacy of wire [including electronic] and oral communications."[27]

In 2001, the Supreme Court directly addressed the application of § 2511(1)(c) where the eavesdropper and discloser are different parties.[28] In *Bartnicki*, a divided Court held that truthful information of "public concern" that is originally obtained

---

[25] Pub. L. No. 90-351, 82 Stat. 197 (1968). The wiretapping provisions of the Act are codified at 18 U.S.C. §§ 2510–22 (2012).

[26] *See* 18 U.S.C. § 2511(1)(c) (2012). The original 1968 text covered only "wire or oral communication[s]." The 1968 version of the subsection read:

> [A]ny person who . . . willfully discloses, or endeavors to disclose, to any other person the contents of any wire or oral communication, knowing or having reason to know that the information was obtained through the interception of a wire or oral communication in violation of this subsection . . . shall be fined not more than $10,000 or imprisoned not more than five years, or both.

Omnibus Crime Control and Safe Streets Act (Wiretap Act), Pub. L. No. 90-351, 82 Stat. 197 (1968). As technology evolved, Congress extended the protections to electronic and computer communications. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848. The most current version of § 2511(1)(c) reads:

> [A]ny person who . . . intentionally discloses, or endeavors to disclose, to any other person the contents of any *wire, oral, or electronic communication*, knowing or having reason to know that the information was obtained through the interception of a *wire, oral, or electronic communication* in violation of this subsection . . . shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5) (emphasis added).

Finally, § 2120 authorizes a private cause of action for suit under § 2511, authorizes equitable relief where necessary, and sets forth a statutory scheme for calculating damages. *See* § 2520(a)–(c).

[27] S. REP. NO. 90-1097, at 37 (1968).

[28] *See* Bartnicki v. Vopper, 532 U.S. 514 (2001).

illegally, and then published by a third party unrelated to the initial theft, is First Amendment protected.[29]

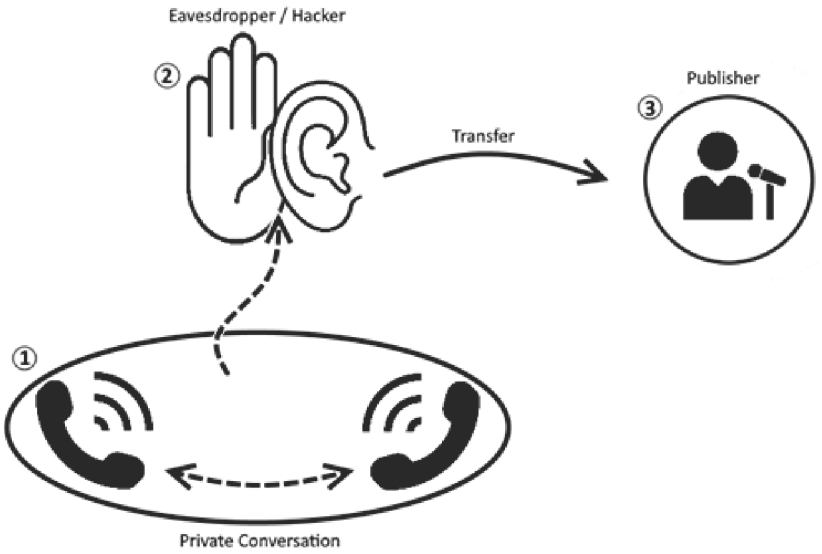

Fig. 1[30]

It is helpful to understand the background of the case. The dispute leading to *Bartnicki* involved an intercepted cell phone conversation.[31] Between 1992 and 1994, the Wyoming Valley West School District, just outside Wilkes-Barre, Pennsylvania, was engaged in a contentious contract negotiation with the district's Teachers' Union.[32] In a May 1993 cell phone call, plaintiff-petitioners Gloria Bartnicki, Chief Union Negotiator, and Anthony Kane, Jr., Union President, were discussing the ongoing contract negotiations.[33] During their private phone conversation, Kane said, "we're gonna have to go to . . . their homes . . . to blow off their front porches, we'll have to do some work on . . . those guys . . . ."[34] Kane then compared union and district negotiating positions, complained of press leaks, and added, "don't discuss the items in public."[35]

It was later discovered that an unknown party had secretly intercepted and tape-recorded the cell phone conversation between Bartnicki and Kane.[36] The anonymous

---

[29] *Id.* at 515.

[30] *See id.*

[31] *See* Bartnicki v. Vopper, 200 F.3d 109, 112–13 (3d Cir. 1999), *cert. granted*, 530 U.S. 1260 (2000).

[32] *Id.*

[33] *Id.*

[34] *Id.* at 113.

[35] *Id.*

[36] *Id.*

eavesdropper then delivered a cassette tape of the conversation to the mailbox of a local anti-teachers' union activist Jack Yocum.[37] Yocum then delivered copies of the tape to two radio stations, WILK and WGBI.[38] The intercepted conversation broadcast repeatedly on local radio stations, aired on local television, and transcripts were published in various local newspapers.[39]

Bartnicki and Kane sued Yocum, WILK, WGBI, and radio D.J. Frederick Vopper under § 2511(1)(c) and the Pennsylvania statutory equivalent.[40] On cross-motions for summary judgment, the District Court granted judgment to Bartnicki and Kane.[41]

On interlocutory appeal, the Third Circuit applied an intermediate scrutiny standard, concluding that § 2511(1)(c) was unconstitutional under the First Amendment because the law was not narrowly tailored to "eliminat[e] . . . demand" for stolen information, and because "the provisions . . . deter significantly more speech than is necessary to serve the government's asserted interest."[42]

At the Supreme Court, however, the majority, led by Justice Stevens, did not explicitly apply intermediate scrutiny. Instead, the Court approached the question as a balancing of constitutional interests. Justice Stevens, joined by Justices Kennedy, Souter, and Ginsburg, with Justices Breyer and O'Connor concurring, recognized a "conflict between interests of the highest order"—namely, privacy and free speech.[43] The majority resolved the conflict in favor of Free Speech interests,[44] invalidating § 2511(1)(c) as applied, along with similar statutes in almost all the states.[45]

Stevens's preferred conception of the flow of information was as a chain of custody[46]: the publisher of information who is itself free from wrongdoing, Stevens concluded, is not to be punished for a prior defect in the chain of custody.[47]

---

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *See id.*; 18 PA. CONS. STAT. § 5703(2) (2018).

[41] *Bartnicki*, 200 F.3d at 113–14. The Defendants did not dispute the facts, and summary judgment turned entirely on the District Court finding that imposing civil liability on the Defendants would not violate the First Amendment. *See id.*

[42] *Id.* at 125–26.

[43] *Bartnicki*, 532 U.S. at 517–18.

[44] As discussed *infra*, however, the *Bartnicki* Court lacked anything nearing a consensus. Justice Breyer concurred in the judgment, joined by Justice O'Connor, arguing that legislatures should have leeway to balance speech and privacy interests. *Id.* at 535, 541 (Breyer, J., concurring in the judgment). Chief Justice Rehnquist dissented, joined by Justice Scalia and Justice Thomas. *Id.* at 541 (Rehnquist, C.J., dissenting).

[45] *See* 18 U.S.C. § 2511(1)(c); *supra* note 15.

[46] *Bartnicki*, 532 U.S. at 528 ("Where the punished publisher of information has obtained the information in question in a manner lawful in itself but from a source who has obtained it unlawfully, may the government punish the ensuing publication of that information based on the defect in a chain?" (quoting Boehner v. McDermott, 191 F.3d 463, 484–85 (D.C. Cir. 1999) (Sentelle, J., dissenting))).

[47] *Id.* at 528–29.

Concurring in the judgment, Justice Breyer advocated application of a balancing test (as he is often wont).[48] The law tolerates restrictions on free speech, Breyer said, where the speaker holds a legitimate interest in maintaining privacy, such as opening mail or trade secret misappropriation.[49] Breyer concurred, however, because the petitioners in this case lacked a "legitimate interest" in concealing their damning conversation from the public.[50] However, Breyer suggested a more tailored statute would pass constitutional muster.[51]

Finally, Chief Justice Rehnquist, joined by Justices Scalia and Thomas, authored a dissent.[52] Rehnquist argued that, because the statute was content-neutral, intermediate scrutiny applied.[53] In Rehnquist's judgment, the prohibition on third-party publication was narrowly tailored to advance the government's legitimate interest in protecting private speech.[54] Rehnquist's dissent presaged the thesis of this Note, arguing that advances in technology place private conversations at exceptional risk of interception and publication.[55]

Since 2001, lower courts have continued to apply § 2511(1)(c) in cases where the disclosure originated from the same party as the wiretap,[56] or where the disclosure originated from a party who conspired with or encouraged the wiretapper.[57] It is, of course, impossible to say how many complaints have *not* been filed since 2001 because of *Bartnicki*.

This Note expresses no opinion on the Court's original 2001 result. Rather, this Note argues that technosocial changes *since* 2001 affect the continuing validity of the earlier holding. Considering the evolution of technology since 2001, more weight must now be placed on privacy interests and more flexibility afforded legislatures to protect such interests. In light of the technosocial change emergent since *Bartnicki*, Justice Stevens's holding should be relaxed.

---

[48] *Id.* at 536 (Breyer, J., concurring in the judgment) ("[T]he key question becomes one of proper fit." (quoting Turner Broad. Sys., Inc. v. F.C.C., 520 U.S. 180, 227 (1997) (Breyer, J., concurring in part))).

[49] *Id.* at 539–40.

[50] *Id.*

[51] *Id.* at 541.

[52] *Id.* at 541–56 (Rehnquist, C.J., dissenting).

[53] *Id.* at 545.

[54] *Id.* at 544.

[55] *Id.* at 542. *See also* Part II *infra*.

[56] *See, e.g.*, Lombardo v. Lombardo, 192 F. Supp. 2d 885 (N.D. Ind. 2002) (applying § 2511(1)(c) in a case where a husband had secretly recorded his wife's phone calls, and later disclosed the recordings in divorce proceedings). After a bench trial, however, the defendant was found liable for the wiretapping but not for the disclosure. *See* Lombardo v. Lombardo, No. 1:99-CV-95, 2005 WL 1459445, at *1 (N.D. Ind. June 20, 2005).

[57] *See* Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007).

II. THE AVAILABILITY, UBIQUITY, AND VARIETY OF TECHNOLOGY HAS CHANGED DRAMATICALLY SINCE *BARTNICKI*, LEAVING PRIVATE INFORMATION FAR MORE VULNERABLE

Chief Justice Rehnquist's prescient dissenting opinion articulates the problem[58]:

> Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations.[59]

This argument has grown far stronger since *Bartnicki* was decided.

A. Today There Are Far More Means and Opportunities to Capture Private Communications and Information than Existed in 2001

If true in 2001, Chief Justice Rehnquist's fears about technology have borne further since then: about four billion gigabytes of data crisscross the internet per day,[60] much without the knowledge or consent of the communicant.[61] Today's technosocial environment presents communicants with a thicket of often subversive data collection, storage, and machine learning.[62]

The facts giving rise to *Bartnicki* occurred in May 1993.[63] In 1994 (the earliest year for which I could find available data), there were an estimated 4.7 million internet subscriptions worldwide.[64] In 1993, there were an estimated 34 million cell

---

[58] *Bartnicki*, 532 U.S. at 541 (Rehnquist, C.J., dissenting). *See also* Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 44 (Ct. App. Minn. 2009) ("A town crier could reach dozens, a handbill hundreds, a newspaper or radio station tens of thousands, a television station millions, and now a publicly accessible webpage can present the story of someone's private life . . . to more than one billion Internet surfers worldwide.").

[59] *Bartnicki*, 532 U.S. at 541 (Rehnquist, C.J., dissenting).

[60] *See* CISCO, *supra* note 2. As explained in the Introduction of this Note, four billion gigabytes of data is equivalent to about 200,000 years of DVD-quality video. *See* PEARSON, *supra* note 2.

[61] *See, e.g.*, Nick Douglas, *How Apps Use Your Photos to Track Your Location*, LIFEHACKER (Oct. 24, 2017), https://lifehacker.com/how-apps-use-your-photos-to-track-your-location-1819802266 [https://perma.cc/BW3V-XVBE].

[62] *See, e.g.*, Sarah Perez, *Facebook Is Pushing its Data-Tracking Onavo VPN Within its Main Mobile App*, TECH CRUNCH (Feb. 12, 2018), https://techcrunch.com/2018/02/12/facebook-starts-pushing-its-data-tracking-onavo-vpn-within-its-main-mobile-app/ [https://perma.cc/BAC8-VNFS] (describing how Facebook's "Onavo Protect" VPN software—customarily a platform used for information privacy—is in fact collecting data on its users).

[63] 532 U.S. at 512–18.

[64] *See* NAT'L RESEARCH COUNCIL, THE UNPREDICTABLE CERTAINTY: INFORMATION INFRASTRUCTURE THROUGH 2000 187 (1996).

phone subscribers worldwide.[65] Today, there are an estimated 920 million broadband internet subscriptions,[66] representing 3.55 billion people.[67] As early as 2009, the number of individual devices connected to the internet surpassed the number of people on Earth.[68] As of 2020, there will be about 50 billion connected devices—about six for every woman, man, and child on Earth.[69] In 2015, an estimated 206 billion emails changed hands each day worldwide[70]—enough for every person alive to send about 27 emails daily.[71] These connections and exchanges of information contain, hold, and may reveal, "the privacies of life."[72]

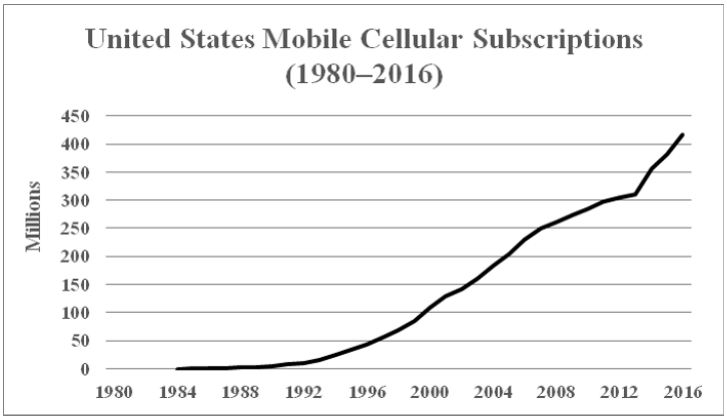

Fig. 2[73]

---

[65] *See Mobile Cellular Subscriptions*, WORLD BANK DATA (2016), https://data.worldbank.org/indicator/IT.CEL.SETS?end=2016&start=1993 [https://perma.cc/V3GA-XGP3].

[66] *See Fixed Broadband Subscriptions*, WORLD BANK DATA (2016), https://data.worldbank.org/indicator/IT.NET.BBND [https://perma.cc/BQX3-Y8C7].

[67] *See Global and Regional ICT Data*, ITU (2017), https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx [https://perma.cc/DVG3-UMJP]. For another estimate see *Internet Usage Statistics: The Internet Big Picture*, INTERNET WORLD STATISTICS (2018), http://www.internetworldstats.com/stats.htm [https://perma.cc/Z8ZH-ARUJ] (estimating 4.2 billion global internet users, representing 54.4 percent of the world population).

[68] *See* FTC, *Internet of Things: Privacy & Security in a Connected World* I (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-November-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/RVM9-YNPT].

[69] *Id.*

[70] Radicati Group, *Email Statistics Report 2015–2019* (Mar. 2015), http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf [https://perma.cc/2YSD-XYT3].

[71] *See U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/popclock/ [https://perma.cc/C6GB-QZ3J] (last visited Oct. 15, 2018) (offering an up-to-the-second global human population estimate).

[72] Boyd v. United States, 116 U.S. 616, 630 (1886) (holding that compulsory production of private papers amounts to a search or seizure within the meaning of the Fourth Amendment).

[73] For source of graph data, see *Mobile Cellular Subscriptions*, *supra* note 65.

Not only is the *volume* of electronic information far greater than ever before, the scope is greater too:

- Information changes hands via phone call, text message, voicemail, email, Facebook, Twitter, Instagram, Snapchat, online dating apps, in-game chat, and more.
- With the onset of the so-called "internet of things," servers now have access to web-connected PCs, cell phones, tablet computers, televisions, cars,[74] videogame consoles, ovens, thermostats, clocks, cameras, wristwatches, speakers, light bulbs, nightlights, light switches, air filters, air vents, garage door openers, herb gardens, exercise bracelets, bathroom scales, smoke detectors, doorbells, door locks, baby monitors, beds, lawn sprinklers, refrigerators, blenders, coffee makers, blood pressure monitors, and even fish finders, breathalyzers, propane tanks, and 9-volt batteries.[75]
- One car industry organization estimates that by 2020, 90 percent of consumer vehicles will be web-connected.[76]
- As of 2018, 33 million American homes are equipped with a "smart speaker"—an always-on artificially intelligent web-connected listening device[77]—a number forecast to more than double by the end of 2018.[78]

The ubiquity of available data exceeds the reasonable expectations of the public regarding the privacy and security of information—data are vulnerable that many

[74] Following a story about hackers assuming remote control of a web-connected vehicle, the Senate introduced a bill seeking to protect drivers. *See* Tom Risen, *Would Your Smart Car Brake for Hackers?*, U.S. NEWS & WORLD RPT. (July 23, 2015, 2:31 PM), https://www.usnews.com/news/articles/2015/07/23/can-hackers-really-target-your-smart-car [https://perma.cc/MUM2-772R]; Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. (2015). This bill died in the committee. It required vehicles to adopt "isolation measures" between "critical" and "noncritical" software, based on rules set forth by the Federal Trade Commission. *Id. See also* SPY Car Study Act of 2017, H.R.701, 115th Cong. (2017) (directing the National Highway Traffic Safety Administration to conduct a study to determine appropriate cybersecurity standards for motor vehicles).

[75] For a list including the above products, see *Postscapes*, https://www.postscapes.com/categories/#consumer [https://perma.cc/HYQ5-FUYR] (last visited Oct. 15, 2018). For readers skeptical of the existence of web-connected batteries, see *Roost Wi-Fi Battery for Smoke and CO Alarms,* ROOST, https://www.getroost.com/product-battery [https://perma.cc/TQL7-SKNL] (last visited Oct. 15, 2018).

[76] *See* CONNECTED CAR INDUSTRY REPORT 2013 9, TELEFONICA (2013), http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf [https://perma.cc/A356-4TZU].

[77] *See* THE 2017 VOICE REPORT EXECUTIVE SUMMARY 4, VOICELABS.CO (Jan. 15, 2017), https://s3-us-west-1.amazonaws.com/voicelabs/report/vl-voice-report-exec-summary_final.pdf [https://perma.cc/79MS-8697].

[78] *See* Anick Jesdanun, *Smart Homes: Not Just for Tech Geeks Anymore*, ASSOCIATED PRESS (Dec. 28, 2017), https://apnews.com/af20a3f73e5b41068bbb91cf87e4ee98 [https://perma.cc/4XX9-TDHZ].

people are not even aware exist.[79] Experts now say data available from existing smartphone sensors can be used to infer a user's mood, stress, personality type, gender, marital status, job status, age, mental illness, smoking habits, physical activity, and overall movement.[80]

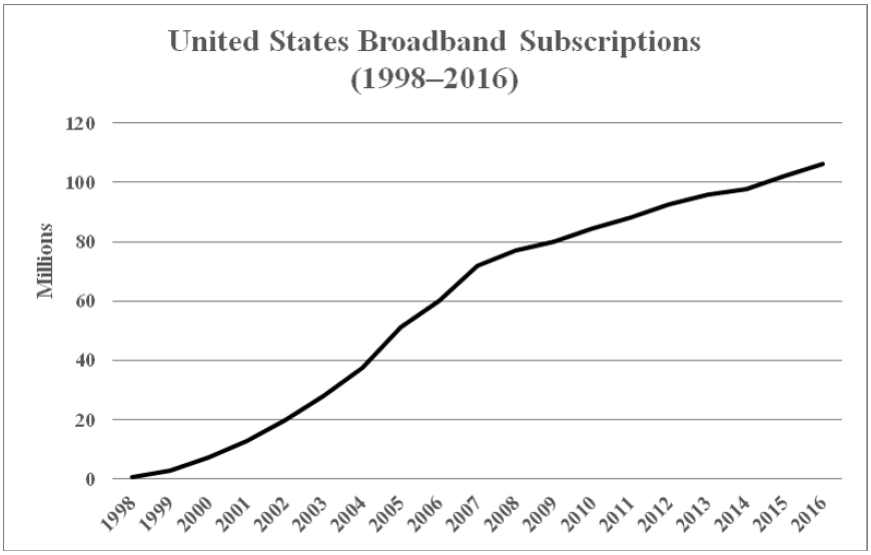

Fig. 3[81]

Where Justice Stevens saw a "conflict . . . of the highest order" between free speech and privacy interests,[82] the massive growth in communications and data technologies now overwhelms privacy interests such that revisiting *Bartnicki* is justified. Recall the scenario that led to *Bartnicki*: in 1993, an unknown person tape-recorded a sensitive cell phone conversation, mailed the cassette to a sympathetic activist, and the tape was then delivered to radio stations who aired it.[83] This series of acts required substantial motive, premeditation, planning, and execution.

---

[79] *See, e.g.*, Timothy R. Graeff & Susan Harmon, *Collecting and Using Personal Data: Consumers' Awareness and Concerns*, 19 J. CONSUMER MKTG. 302 (2002) (showing consumers are generally unaware how "discount loyalty card" programs track their personal information).

[80] *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 115–16 (2014).

[81] *See Fixed Broadband Subscriptions*, *supra* note 66.

[82] Bartnicki v. Vopper, 532 U.S. 514, 518 (2001).

[83] *See id.* at 518–19. The history of Wiretap Act litigation reveals another high-profile case that predates *Bartnicki*, the procedurally complex *Boehner v. McDermott*. 191 F.3d 463 (D.C. Cir. 1999) (upholding judgment against Congressman Jim McDermott, who in 1996 arranged to acquire a tape of a private wiretap of Congressman John Boehner). Upon the ruling in *Bartnicki*, the Supreme Court vacated the D.C. Circuit's judgment. McDermott v. Boehner, 532 U.S. 1050 (2001). Upon remand, the District Court distinguished *Bartnicki* because Rep.

Now imagine a similar scenario in 2018—how might it play out differently? A wrongdoer still could audio-record the conversations. Rather than physically deliver a cassette though, an audio recording can now be digitized and delivered anonymously in a matter of minutes to an arbitrary number of recipients, to an audience of arbitrary size and scope.[84]

Instead of recording the audio of a private conversation, such a modern wrongdoer could steal and crack a smartphone or computer hack into an email account, hack into a "cloud" account, hack into a voicemail account, intercept WiFi signal communications, or "phish" for bank or other personal information.[85] Most of this information is in the custody of some third-party entity other than the subject.[86]

Notwithstanding illicit hacking, the volume and breadth of personal identifying information freely available is remarkable. One's home address is often ascertainable online.[87] Court documents, records, and wills are readily available and easily retrievable.[88] One's ancestry and immigration history are discoverable.[89] In a recent case, a journalist was able to easily discover that a prominent Fox News commentator is the descendant of a North Dakotan man who was accused of lying on his immigration papers in 1909.[90] In March 2017, a journalist needed only four hours using completely

---

McDermott had knowledge of the illegal wiretap. Boehner v. McDermott, 332 F. Supp. 2d 149 (D.D.C. 2004). The D.C. Circuit later affirmed. Boehner v. McDermott, 484 F.3d 573 (D.C. Cir. 2007). This case illustrates exactly the sort of behavior the Wiretap Act is intended to deter.

[84] *See, e.g.*, Tim Nudd, *The Story Behind the Pants-Soiling 'Rings' Prank That Has 200 Million Views in 24 Hours*, ADWEEK (Jan. 24, 2017), http://www.adweek.com/creativity/story-behind-pants-soiling-rings-prank-has-200-million-views-24-hours-175720/ [https://perma.cc/5EGX-N8AN] (describing a marketing campaign through which a viral YouTube video was viewed over 200 million times within a day of uploading).

[85] *See, e.g.*, Charles Arthur, *Naked Celebrity Hack: Security Experts Focus on iCloud Backup Theory*, GUARDIAN (Sept. 1, 2014), https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence [https://perma.cc/U678-FUDV].

[86] *See id.* (discussing how hackers accessed the celebrity photos possibly through iCloud backups or Dropbox).

[87] *See* Charlie Burton, *How to Find Anyone Online*, WIRED (May 3, 2017), http://www.wired.co.uk/article/how-to-find-anyone [https://perma.cc/58RK-J3EK] (explaining how to track someone's location online).

[88] *See, e.g.*, Last Will and Testament of John F. Kennedy, Jr., https://www.livingtrustnetwork.com/estate-planning-center/last-will-and-testament/wills-of-the-rich-and-famous/last-will-and-testament-of-john-kennedy-jr.html [https://perma.cc/WUD7-65DS]. The website hosts the wills of, among others, Diana, Princess of Wales, Walt Disney, James Gandofini, Michael Jackson, and Whitney Houston. *See Wills of the Rich and Famous*, LIVING TRUST NETWORK, https://www.livingtrustnetwork.com/estate-planning-center/last-will-and-testament/wills-of-the-rich-and-famous.html [https://perma.cc/744P-HA9N].

[89] *See, e.g.*, Jennifer Mendelsohn, *Tomi Lahren, Meet The Great Great Grandfather Prosecuted For Forging His Citizenship Papers!*, WONKETTE (Sept. 7, 2017, 11:29 AM), https://wonkette.com/622623/tomi-lahren-meet-the-great-great-grandfather-prosecuted-for-forging-his-citizenship-papers [https://perma.cc/56ZB-J9NM].

[90] *See id.*

public, conventional tools and platforms to discover then–FBI Director James Comey's pseudonymous Twitter account.[91] In October 2017, Comey confirmed the unearthed account was in fact his.[92] Even the Pentagon cannot keep up. In January 2018, an intelligence analyst was able to use publicly available fitness tracker location data to map secret military bases in Afghanistan, Syria, the Falkland Islands, and Somalia.[93]

B. Actual Instances of Compromise and Distribution of Private Information Are Common

These privacy concerns are hardly theoretical. In 2012, the British newspaper, *News of the World*, became embroiled in scandal when it was revealed that journalists were hacking celebrities' and politicians' cell phones, computers, and voicemail inboxes.[94] Over twenty journalists were charged with crimes.[95] There were countless public hearings and a major government inquiry into ethical conduct in U.K. journalism.[96]

While *Bartnicki* does not apply directly to a circumstance where the thief is *also* the publisher,[97] under the holding of *Bartnicki*, in the United States, the *News of the World*'s journalists—or any motivated individual—could have laundered the stolen information, for example, if they had simply passed it to another newspaper.

Countless other specific instances in the past several years illustrate the vulnerability of private information, including private speech which is published to the detriment

---

[91] Ashley Feinberg, *This Is Almost Certainly James Comey's Twitter Account*, GIZMODO (Mar. 30, 2017), https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641 [https://perma.cc/73UK-RRFY] ("[I]t only took me about four hours of sleuthing to find Comey's account, which is not protected.").

[92] *See* Reinhold Niebuhr (@FormerBu), TWITTER (Oct. 23, 2017, 8:34 AM), https://twitter.com/FormerBu/status/922486295611371526 [https://perma.cc/8SEJ-TSST] (revealing a photograph of Comey, implying Comey operates the account); Benjamin Wittes (@benjaminwittes), TWITTER (Oct. 23, 2017, 8:37 AM), https://twitter.com/benjaminwittes/status/922487180756385793 [https://perma.cc/5MRM-H566] (personal friend of Comey confirming the anonymous account @FormerBu belongs to Comey).

[93] *See* Jon Fingas, *Strava Fitness Tracking Data Reveals Details of Secret Bases*, ENGADGET (Jan. 28, 2018), https://www.engadget.com/2018/01/28/strava-fitness-tracking-data-reveals-details-of-secret-bases/ [https://perma.cc/793E-A38P]; Alex Hern, *Fitness Tracking App Strava Gives Away Location of Secret US Army Bases*, GUARDIAN (Jan. 28, 2018), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases [https://perma.cc/8UDC-2JUL].

[94] *See* Alan Cowell, *At British Inquiry, Rupert Murdoch Apologizes Over Scandal*, N.Y. TIMES (Apr. 26, 2012), http://www.nytimes.com/2012/04/27/world/europe/rupert-murdoch-testimony-leveson-inquiry-day-2.html?_r=2&hp.

[95] *Id.* ("Twenty . . . have been arrested in separate inquiries into phone and computer hacking by journalists at News International.").

[96] *See The Leveson Inquiry, An Inquiry Into The Culture, Practices and Ethics Of The Press*, U.K. GOV'T (Nov. 2012), https://www.gov.uk/government/publications/leveson-inquiry-report-into-the-culture-practices-and-ethics-of-the-press [https://perma.cc/6U4X-C398].

[97] *See* Bartnicki v. Vopper, 532 U.S. 514, 515–16. Justice Stevens explicitly avoids addressing such a situation. *Id.*

of the speaker. In 2008, a "hacker" (of a sort) abused a flaw in a password reset feature and breached the email account of then-Vice-Presidential nominee and Alaska governor Sarah Palin.[98] The hacker was charged for the hack itself and the obstruction of justice and eventually sentenced to a year imprisonment.[99] In late 2014, a single hacker breached the iCloud accounts of numerous celebrities, copied privately taken sexually explicit photographs and videos, and distributed the photographs on several internet message boards.[100] That same year, a group identified as "Guardians of Peace" hacked the film studio Sony Pictures and leaked email correspondence of executives, employees, actors, and their families; salary information; complete copies of unreleased films; and other data.[101] And in early 2017, a hacker breached the email account of celebrity footballer David Beckham and stole personal tax information.[102] The information came into possession of news outlets.[103] A U.K. court first enjoined publication, but later reversed its injunction as moot; the emails had already leaked through non-U.K. publications.[104]

---

[98] *See* M.J. Stephey, *Sarah Palin's E-Mail Hacked*, TIME (Sept. 17, 2008), http://content.time.com/time/politics/article/0,8599,1842097,00.html [https://perma.cc/4AWC-TZXW]; Kim Zetter, *Palin E-Mail Hacker Says It Was Easy*, WIRED (Sept. 18, 2008), https://www.wired.com/2008/09/palin-e-mail-ha/ [https://perma.cc/2YZQ-GZRG].

[99] *See* Kim Zetter, *Sarah Palin E-Mail Hacker Sentenced to 1 Year in Custody*, WIRED (Nov. 12, 2010), https://www.wired.com/2010/11/palin-hacker-sentenced/ [https://perma.cc/V36W-MHX6]; Computer Fraud and Abuse Act, 18 U.S.C. § 1030; 18 U.S.C. § 1519 (destroying records in a federal investigation is obstruction of justice); Terry Baynes, *Sarah Palin Email Hacker Loses Appeal*, REUTERS (Jan. 30, 2012), https://www.reuters.com/article/us-palin-hacking/sarah-palin-email-hacker-loses-appeal-idUSTRE80T1UQ20120130 [https://perma.cc/6NMM-G4PN]; United States v. Kernell, No. 08-CR-142, 2010 WL3937421 (E.D. Tenn., Sept. 23, 2010).

[100] *See* Arthur, *supra* note 85; *see also* Tom Sykes, *Celebrity Nude Photo Hack: Images of Miley Cyrus, Kristen Stewart, Tiger Woods and More Leak Online*, DAILY BEAST (Aug. 22, 2017), https://www.thedailybeast.com/celebrity-nude-photo-hack-images-of-miley-cyrus-kristen-stewart-tiger-woods-and-more-leak-online [https://perma.cc/3PKZ-CW9D] (describing a similar mass-theft of sexual photographs in August 2017).

[101] Gabi Siboni & David Siman-Tov, *Cyberspace Extortion: North Korea Versus the United States*, INSS INSIGHT 646 (Dec. 23, 2014), http://www.inss.org.il/wp-content/uploads/sites/2/systemfiles/SystemFiles/No.%20646%20-%20Gabi%20and%20Dudi%20for%20web.pdf [https://perma.cc/5SMC-8TZB]. Most analysts agree the perpetrators were working for or at the behest of North Korea. *Id. See also* Michael S. Schmidt et al., *F.B.I. Says Little Doubt North Korea Hit Sony*, N.Y. TIMES (Jan. 7, 2015), https://www.nytimes.com/2015/01/08/business/chief-says-fbi-has-no-doubt-that-north-korea-attacked-sony.html.

[102] *See, e.g.*, Peter Preston, *We Need to Talk About Stolen Goods—And That Includes Hacked Emails*, GUARDIAN (Feb. 12, 2017), https://www.theguardian.com/media/2017/feb/12/beckham-emails-media-law-privacy-hacking-leveson [https://perma.cc/P43N-W5T2] ("As they stand, any mafia hacker in nether Moscow has a license to trawl through the email accounts of the rich and famous until they strike gold . . . .").

[103] *See id.*

[104] *See id.*

Akin to the "third-party" scenario in *Bartnicki*, the radical transparency website *Wikileaks* has published stolen classified documents and sensitive electronic correspondence in several high-profile cases since 2009. Although it is not known whether *Wikileaks* was soliciting or conspiring with the hackers and thieves, they certainly published information that, consistent with the language of § 2511(1)(c), they knew or should have known was misappropriated or stolen.[105]

Wikileaks published the stolen Sarah Palin emails, described previously,[106] hundreds of thousands of stolen pager messages sent on September 11, 2001,[107] and tens of thousands of military assessments and State Department cables.[108] In 2016, *Wikileaks* published two massive leaks of *private* email correspondence: they published

---

[105] *See* § 2511(1)(c); Charlie Savage, *U.S. Tries to Build Case for Conspiracy by WikiLeaks*, N.Y. TIMES (Dec. 15, 2010), http://www.nytimes.com/2010/12/16/world/16wiki.html. *Wikileaks* launched in late 2006, billing itself as a radical civil libertarian and transparency organization. *See generally* DANIEL DOMSCHEIT-BERG, INSIDE WIKILEAKS (Jefferson Chase trans., Crown Publ'g) (2011). Whatever one's personal views of *Wikileaks*' purported mission, there is no doubt *Wikileaks* habitually posts information that was obtained through criminal activity, such as from hacking. *See, e.g.*, *Sarah Palin Yahoo Account 2008*, WIKILEAKS (Sept. 17, 2008), https://wikileaks.org/wiki/Sarah_Palin_Yahoo_account_2008 [https://perma.cc/64QE-BBYX]; *Sony Emails*, WIKILEAKS (Apr. 16, 2015), https://wikileaks.org/sony/emails/ [https://perma.cc/ZC7P-8DWN].

[106] *See Sarah Palin Yahoo Account 2008*, *supra* note 105; M.J. Stephey, *Sarah Palin's E-Mail Hacked*; Kim Zetter, *Palin E-Mail Hacker Says It Was Easy*, *supra* note 98.

[107] *See 9/11 Pager Data*, WIKILEAKS (Nov. 25, 2009), https://911.wikileaks.org/ [https://perma.cc/NM7C-AWAY]; Jennifer Millman, *Analysis of 9/11 Pager Data Paints Chilling Picture*, NBC NEWS (Dec. 1, 2009), https://www.nbcnewyork.com/news/local/Analysis-of-911-Pager-Data-Paints-Chilling-Picture-78219132.html [https://perma.cc/4U3K-2PHX]. The thief of the pager messages has still not been identified. *See* Evan Hansen, *Manning-Lamo Chat Logs Revealed*, WIRED (July 13, 2011), https://www.wired.com/2011/07/manning-lamo-logs/ [https://perma.cc/TD8P-JY28]. Logs suggest the pager messages were stolen from an NSA database. *Id.*

[108] *See Baghdad War Diary*, WIKILEAKS (Oct. 22, 2010), https://wikileaks.org/irq/ [https://perma.cc/5SKQ-2VV2]; SPIEGEL Staff, *Greatest Data Leak in US Military History*, DER SPIEGEL (Oct. 22, 2010, 10:52 PM), http://www.spiegel.de/international/world/the-wikileaks-iraq-war-logs-greatest-data-leak-in-us-military-history-a-724845.html [https://perma.cc/RPJ2-GDAU]. In January 2010, United States Army intelligence analyst, presently known as Chelsea E. Manning, *see* Verónica Bayetti Flores, *Manning Announces She is Transitioning*, FEMINISTING (Aug. 22, 2013), http://feministing.com/2013/08/22/manning-announces-she-is-transitioning/ [https://perma.cc/VYA3-ETE4], downloaded classified documents and videos, and on February 3, 2010 passed the information to *Wikileaks*; Memorandum (author classified), *Statement in Support of Providence Inquiry—U.S. v. Private First Class (PFC) Bradley E. Manning (U)*, Jan. 29, 2013. Manning continued to pass additional documents to *Wikileaks* over the following weeks. *See* Steven Lee Myers, *Charges for Soldier Accused of Leak*, N.Y. TIMES (July 6, 2010), http://www.nytimes.com/2010/07/07/world/middleeast/07wikileaks.html. From this leak, between February 18, 2010 and September 1, 2011, Wikileaks gradually published U.S. government profiles of foreign leaders and diplomats; a video of a July 12, 2007 airstrike in Iraq which killed and injured journalists and civilians; 91,731 classified Afghanistan War military reports; 391,832 classified Iraq War military reports; 251,287 State Department cables; and 779 classified Guantánamo Bay files.

thousands of Democratic National Committee documents, and, separately, thousands of emails from the personal Gmail account of Hillary Clinton's presidential campaign chairman, John Podesta.[109]

Assuming, for the sake of argument, that *Wikileaks* was only a passive recipient (and notwithstanding jurisdictional issues), under *Bartnicki*, the victims of these hacks, such as Podesta, would almost certainly have no recourse against *Wikileaks* under the Wiretap Act to prevent or seek compensation for publication of these private communications.[110]

Notwithstanding these specific examples of communications breach, data also show significant number of data breaches against the public generally. In 2015, Americans suffered approximately 3 million economic cybercrimes.[111] The European Union, meanwhile, estimates 12 percent of European Union citizens have experienced personal online fraud.[112]

Not all of the above examples necessarily implicate the *Bartnicki* holding directly. However, these examples illustrate that thefts of stored electronic communications and subsequent publication are already a serious problem.

C. Breaches and Thefts Are Likely to Continue as New Software Vulnerabilities Come to Light Regularly

New vulnerabilities and security flaws seem to come to light every week. Software firms have a powerful incentive to develop and sell products to the public

---

[109] Specifically, on July 22, 2016, *Wikileaks* published 19,252 emails and 8,034 email attachments, which had been exchanged between seven Democratic National Committee senior staff members between January 2015 and May 2016. Then, beginning October 7, 2016, *Wikileaks* began publishing nearly 20,000 private emails from Podesta's account. Investigators determined that Podesta's email account had been compromised through a "phishing" attack in March 2016. *See* Raphael Satter, *Inside Story: How Russians Hacked the Democrats' Emails*, ASSOCIATED PRESS (Nov. 4, 2017), https://www.apnews.com/dea73efc01594839957c3c9a6c962b8a [https://perma.cc/CSP5-WC8N]. The United States has been specifically investigating throughout this period since 2009 whether *Wikileaks* was a passive recipient of misappropriated information, or actively soliciting or conspiring. *See* Savage, *supra* note 105.

[110] *See* Bryan Burrough, Sarah Ellison & Suzanna Andrews, *The Snowden Saga: A Shadowland of Secrets and Light*, VANITY FAIR (May 2014), https://www.vanityfair.com/news/politics/2014/05/edward-snowden-politics-interview [https://perma.cc/5AW6-W9VN]; *see also* Opening Brief in Support of Defendant Donald J. Trump for President, Inc.'s Motion to Dismiss, Cockrum v. Donald J. Trump for President, Inc., No. 3:18-cv-00484 at 4–9 (E.D. Va. Oct. 8, 2018), ECF No. 23 (arguing the First Amendment, as interpreted in *Bartnicki*, protects the Trump Campaign's reproduction and dissemination of stolen DNC emails).

[111] Michael Levi, *Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues*, 67 CRIME L. SOC. CHANGE 3, 11 (2017). Levi argues United States cybercrime data collection and reporting is grossly inadequate "as if the nation was stuck in the Dillinger Days." *Id.* The FBI received 288,012 cybercrime complaints in 2015, and the FBI estimates fewer than 10 percent of victims report cybercrimes, meaning one could infer Americans suffered about 3 million cybercrimes in 2015. *See id.*

[112] *Id.* at 5.

but little incentive to discover and patch vulnerabilities which are very difficult and expensive to find.[113] In many cases, the developer no longer exists or has discontinued product support.[114]

Hackers, on the other hand, are innumerable and possess a major incentive to search for vulnerabilities. So-called "zero day" flaws are those discovered but of which the software developer is unaware.[115] For example, residential and commercial WiFi routers connect to users' personal devices on what is typically an encrypted local area network, or WLAN.[116] The encryption standard called Wireless Equivalent Privacy (WEP) is still available on most wireless routers (not generally by default setting).[117] However, as early as October 2000,[118] serious flaws with WEP were discovered.[119]

In the wake of the WEP failure, the wireless encryption standard was replaced with Wi-Fi Protected Access (WPA) and later WPA2,[120] which developed a "gold

---

[113] *See* Stephen Kampff, *Should We Be Paying for Firmware Updates?*, FSTOPPERS (Jan. 10, 2017), https://fstoppers.com/originals/should-we-be-paying-firmware-updates-161007 [https://perma.cc/K9YB-XD25].

[114] When unsupported software is maintained by private users in the public, it has its own name: "abandonware." *See, e.g.*, Brad King, *Abandonware: Dead Games Live On*, WIRED (Jan. 19, 2002, 2:00 AM), https://www.wired.com/2002/01/abandonware-dead-games-live-on/ [https://perma.cc/5R9F-ZE2R]. After Microsoft discontinued product support for Windows 98, fans in the user community privately developed and launched their own software patches. *See* Hans-Christian Dirscherl, *Nicht tot zu Kriegen: Win 98 Service Pack 2.1* [*Not to be Killed: Win 98 Service Pack 2.1*], PC WELT (Nov. 29, 2005, 10:24 AM), https://www.pcwelt.de/news/Nicht-tot-zu-kriegen-Win-98-Service-Pack-2-1-402036.html [https://perma.cc/J8P7-CD8W].

[115] *See How Do Zero-Day Vulnerabilities Work: #30SecTech*, SYMANTEC SECURITY CTR., https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html [https://perma.cc/J5G2-AMNF] (last visited Oct. 15, 2018); *see also* Kim Zetter, *Hacker Lexicon, What is a Zero Day?*, WIRED (Nov. 11, 2014, 6:30 AM), https://www.wired.com/2014/11/what-is-a-zero-day/ [https://perma.cc/97VD-CZXN].

[116] *See* Dong Ngo, *Home Networking: Everything You Need to Know*, CNET (Feb. 15, 2017, 11:31 AM), https://www.cnet.com/how-to/home-networking-explained-part-1-heres-the-url-for-you/ [https://perma.cc/K2GJ-PFJA].

[117] *See* Michael Horowitz, *WiFi Over-The-Air Encryption: WEP, WPA and WPA2*, ROUTER SECURITY (July 13, 2015), https://routersecurity.org/wepwpawpa2.php [https://perma.cc/G5K9-LGXW].

[118] *Wireless Research*, UNIV. MD., http://www.cs.umd.edu/~waa/wireless.html [https://perma.cc/F9X2-95A3] (last visited Oct. 15, 2018).

[119] *See Security of the WEP Algorithim*, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html [https://perma.cc/ZT54-6KYK] (last visited Oct. 15, 2018); *see also* Kevin Beaver et al., *Understanding WEP Weaknesses*, DUMMIES.COM, http://www.dummies.com/programming/networking/understanding-wep-weaknesses/ [https://perma.cc/97BV-7EYP]; Gina Trapani, *How to Crack a Wi-Fi Network's WEP Password with BackTrack*, LIFEHACKER (Oct. 28, 2011), https://lifehacker.com/5305094/how-to-crack-a-wi-fi-networks-wep-password-with-backtrack [https://perma.cc/4EVT-EKU7] (describing a simple software tool for automatically hacking WEP-encrypted WLANs).

[120] *See* Horowitz, *supra* note 117.

standard" reputation for residential and commercial network encryption.[121] However, it was revealed in October 2017 that, like WEP before it, WPA2 is catastrophically flawed and easily hacked.[122] Since the replacement of WEP, tens of millions of WPA/WPA2-encrypted devices entered the market.[123] This flaw is likely to precipitate numerous breaches.[124]

In April 2014, a major security flaw in OpenSSL (the secure communications software that connects most computers to servers on the internet) was uncovered.[125] Known as "Heartbleed," the bug existed in the software for a full two years before it

---

[121] *Id.*

[122] Lily Hay Newman, *The 'Secure' Wi-Fi Standard Has a Huge, Dangerous Flaw*, WIRED (Oct. 16, 2017, 11:03 AM), https://www.wired.com/story/krack-wi-fi-wpa2-vulnerability/ [https://perma.cc/9M4M-94GB].

[123] *Id.*

[124] Such flawed WLAN security has already proven a serious danger. In 2007, the WLAN of retailer TJX Companies, Inc., which operates T.J. Maxx, Marshalls, and HomeGoods stores (among others) was breached, and 96 million credit card accounts were stolen. *See* Kim Zetter, *TJX Failed to Notice Thieves Moving 80-Gbytes of Data on Its Network*, WIRED (Oct. 26, 2017,10:18 AM), https://www.wired.com/2007/10/tjx-failed-to-n/ [https://perma.cc/F6N4-HGB9]. The estimated number affected was dramatically revised over the course of investigation. *See* Jaikumar Vijayan, *TJX Data Breach: At 45.6M Card Numbers, It's the Biggest Ever*, COMPUTERWORLD (Mar. 29, 2007, 1:00 PM), https://www.computerworld.com/article/2544306/security0/tjx-data-breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html [https://perma.cc/26U3-2DV7]. Hackers were able to wirelessly install "sniffer" software on TJX's systems using a high-gain antenna mounted to their vehicle, from a distance and without physically handling any TJX hardware inside the stores. *See* Indictment at 3–5, United States v. Gonzalez, No. 08-CR-10223 (D. Mass. Aug. 8, 2008); *see also Antenna Theory for Wardriving and Penetration Testing*, INFOSEC INST. (Jan. 22, 2015), https://resources.infosecinstitute.com/antenna-theory-wardriving-penetration-testing/#gref [https://perma.cc/S28L-49LU]. The hackers' malware captured credit card data as it passed through TJX's network. The hackers were able to easily download customers' names, addresses, social security numbers, and payment card data. *See* In the Matter of The TJX Companies, Inc., No. 072-3055, 2008 WL 3150421, at *2 (F.T.C. 2008). TJX ultimately agreed to a consent order with the federal government, and settled law suits with a class of consumer and with 41 states. *See* W.J. Hennigan, *TJX Agrees to Pay $9.75 Million to Forty-One States in Data Breach Case*, L.A. TIMES (June 24, 2009), http://articles.latimes.com/2009/jun/24/business/fi-tjx24 [https://perma.cc/XC6P-Z83Z]; *see also* Mike Barris, *TJX, MasterCard to Settle Data Breach Lawsuit*, WALL ST. J. (Apr. 2, 2008), https://www.wsj.com/articles/SB120715754287583743 [https://perma.cc/8655-KMKD].

[125] *OpenSSL Heartbleed Vulnerability*, PUB. SAFETY CAN. (Apr. 11, 2014), https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/2014/al14-005-en.aspx [https://perma.cc/MZ35-2TC4]. The Canadian government discovered the flaw after personal identifying information of 900 Canadian taxpayers was stolen from a government database. Pete Evans, *Heartbleed Bug: RCMP Asked Revenue Canada to Delay News of SIN Thefts*, CBC NEWS (Apr. 14, 2014, 8:40 AM), http://www.cbc.ca/news/business/heartbleed-bug-rcmp-asked-revenue-canada-to-delay-news-of-sin-thefts-1.2609192 [https://perma.cc/V5J7-KP2K].

was discovered and patched.[126] The Heartbleed flaw would allow a hacker to capture packets of unencrypted data, typically passwords. Affected websites included Yahoo!, Imgur, Pinterest, Reddit, and Tumblr.[127]

Several other high profile large-scale system breaches due to hidden flaws have been in the news recently:

- In 2011, PlayStation Network was hacked in what was then one of the largest breaches in history, in which 77 million accounts were compromised, and Sony's network downed for 23 days.[128]
- In June 2015, the United States Office of Personnel Management was breached and personal information of 22.1 million current and former federal government employees stolen.[129]
- In July 2015, a hacker group stole over 25 gigabytes of data from Ashley Madison, an online dating website designed for enabling extramarital affairs.[130] The hackers published thousands of lines of user data, including real names, addresses, and credit card information.[131]
- In late 2016, it was determined that internet service company Yahoo! had been massively breached twice, in August 2013 and in late 2014, compromising the data of all three billion Yahoo! users' accounts.[132]

---

[126] R. Seggelmann, M. Tuexen & M. Williams, *Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) Heartbeat Extension*, RFC EDITOR (Feb. 2012), https://www.rfc-editor.org/rfc/rfc6520.txt [doi:10.17487|do:10.17487|RFC6520] [https://perma.cc/557J-TAKS] (describing the extensions to OpenSSL framework that were later discovered in April 2014 to be severely flawed).

[127] Jason Cipriani, *Heartbleed Bug: Check Which Sites Have Been Patched*, CNET (Apr. 9, 2014, 2:54 AM), https://www.cnet.com/how-to/which-sites-have-patched-the-heartbleed-bug/ [https://perma.cc/NX7N-YPAD] (listing the top 100 most-visited sites on the internet and whether they were affected by Heartbleed, and whether they had been patched as of the date of publication).

[128] *See* Letter from Kazuo Hirai, Chairman of the Board of Directors, Sony Computer Entertainment America, to the Honorable Mary Bono Mack and the Honorable K.G. Butterfield, Subcommittee on Commerce, Manufacturing, and Trade (May 3, 2011), copy *available at* https://www.flickr.com/photos/playstationblog/5687531722/in/album-72157626521862165/ [https://perma.cc/U8DG-M59A].

[129] *See* Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say [https://perma.cc/86WG-9N25].

[130] *See* Simon Thomsen, *Extramarital Affair Website Ashley Madison Has Been Hacked and Attackers Are Threatening to Leak Data Online*, BUSINESS INSIDER (July 20, 2015, 4:31 AM), http://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7 [https://perma.cc/2XHH-CYU7].

[131] *Id.*

[132] *See* Robert McMillan & Ryan Knutson, *Yahoo Triples Estimate of Breached Accounts to 3 Billion*, WALL ST. J. (Oct. 3, 2017), https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804 [https://perma.cc/MXQ4-XX2P].

- In July 2016, at least 143 million consumer financial records were stolen from Equifax, a credit ratings agency.[133] The hackers had exploited a vulnerability in Equifax's consumer dispute portal.[134] News outlets reported in February 2018 that the Equifax breach also included tax information and drivers' license data.[135]
- In October 2017, the security firm Kaspersky Labs revealed the existence of security flaws in nine popular online dating sites and apps that allow a hacker to determine a user's real name and location, view photographs, determine page views, and read messages.[136] The potential for extortion and public embarrassment is obvious.

The point of these various examples is not to frighten the reader, but rather to exemplify the reality that billions of private communications change hands each day, and that the systems through which we communicate are almost certainly vulnerable to eavesdropping and theft. The volume and availability of stolen communications will be far greater in 2018 and beyond than when *Bartnicki* was decided in 2001.[137]

---

[133] *See* Lee Mathews, *Equifax Data Breach Impacts 143 Million Americans*, FORBES (Sept. 7, 2017, 10:42 PM), https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/ [https://perma.cc/9QX7-NQPF].

[134] *See id.*; Donna Borak & Kathryn Vasel, *The Equifax Hack Could Be Worse Than We Thought*, CNN MONEY (Feb. 10, 2018, 10:43 AM), http://money.cnn.com/2018/02/09/pf/equifax-hack-senate-disclosure/index.html [https://perma.cc/96A6-2D6B].

[135] *See* Borak & Vasel, *supra* note 134.

[136] *See* Roman Unuchek, Mikhail Kuzen & Sergey Zelenoky, *Dangerous Liaisons: Investigating the Security of Online Dating Apps*, SECURELIST (Oct. 24, 2017, 9:00 AM), https://securelist.com/dangerous-liaisons/ [https://perma.cc/9PF4-X7UT] (describing research regarding network vulnerabilities of Android and iOS versions of nine online dating apps). *Id.* ("We're talking here about intercepting and stealing personal information and the de-anonymization of a dating service that could cause victims no end of troubles—from messages being sent out in their names to blackmail."). For an anecdote about the volume and breadth of data dating sites and apps maintain from their users, see Judith Duportail, *I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets*, GUARDIAN (Sept. 26, 2017, 02:10 AM), https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold [https://perma.cc/XT97-RYWV] (describing a dossier containing details on, among other things, author's Facebook "likes"; Facebook friends; Instagram photos; education; employment history; romantic preferences; sexual preferences; musical tastes; and time, duration, location, and content of conversations).

[137] *See, e.g.*, Dan O'Sullivan, *Dark Cloud: Inside the Pentagon's Leaked Internet Surveillance Archive*, UPGUARD (Apr. 30, 2018), https://www.upguard.com/breaches/cloud-leak-centcom [https://perma.cc/ECN7-ZUTJ] (describing how the Department of Defense collected about 1.8 billion social media posts and inadvertently stored them on public Amazon cloud servers open to worldwide inspection) ("[T]his disparate collection of data appears to constitute an ingestion engine for the bulk collection of internet posts—organizing a mass quantity of data into a searchable form.").

Even the Department of Defense could not anticipate and account for all the data they were sharing.[138]

The Court must take this reality into account when considering what legal tools legislatures should have at their disposal to deter and interdict stolen communications and punish their publication.

D. Evidence Suggests the Public Generally Values Privacy Interests, But That People Are Poor at Assessing Risk and Protecting Themselves

With a rising volume of communications and a range of risks set forth above, one might expect the public to adjust habits and protect themselves. These risks would be theoretically mitigated if communicants were to adjust their behavior accordingly. However, evidence suggests Americans reasonably lack the ability to shield themselves from such data exposure and view loss of information privacy as futile.[139]

Recent polling found 93 percent of adults said controlling who accessed information about them was important.[140] Ninety-one percent of adults agreed that consumers had "lost control" of their personal information.[141] Eighty percent were concerned about how third parties accessed and exploited personal data.[142] Eighty-eight percent agreed "that it would be very difficult to remove inaccurate information about them from online."[143]

Eighty-one percent of surveyed adults considered their personal health information sensitive;[144] 81 percent considered content of telephone conversations sensitive;[145] 77% considered content of email messages sensitive;[146] 75% considered content of text messages sensitive;[147] 75% considered numbers dialed or texted sensitive;[148] and even 66 % considered their birthdate sensitive information.[149] Sixty-one percent of surveyed adults wanted some form of a "right to be forgotten" whereby citizens can command websites and search engines to delete personal information.[150]

---

[138] *See* Hern, *supra* note 93.

[139] *See infra* notes 141–53.

[140] Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [https://perma.cc/P9T4-X5HM] (detailing that 74% out of the 93% considered such control "very important").

[141] Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW INTERNET RES. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ [https://perma.cc/8WC4-JQ59].

[142] *Id.*

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] *U.S. Attitudes Toward the 'Right to Be Forgotten*,' SOFTWARE ADVICE (2014), https://

Despite the expressed concerns, only 30 % of surveyed adults said they had taken at least one step to hide or shield their information.[151] Fifty-four percent considered it would be "somewhat" or "very" difficult to find tools or use strategies to aid them in becoming more private online or when they used their cell phones.[152]

Studies have also shown consumers are poor at weighing available information to assess privacy risks associated with third-party mobile apps.[153] Internet users are not particularly risk averse in their online activities.[154] Qualitative investigation (i.e., subject interviews) has suggested that generally the layperson public only has a vague idea of the architecture of the internet and cell phone networks, and laypeople do not understand well where their data goes and who has access to such data.[155]

The volume and range of information privacy risks have increased dramatically since 2001. Importantly, the public is only vaguely aware of and ill-prepared for the full extent and contours of such risks. The Supreme Court should take this reality into account.

III. THE SUPREME COURT OFTEN REASSESSES ITS HOLDINGS AND PRINCIPLES AS TECHNOLOGY EVOLVES

It is not generally remarkable for the Court to reverse itself or reframe a constitutional question. And the more specific proposition that the Supreme Court should revisit, reverse, or relax its doctrine *because of changes in technology* is neither far-fetched nor new. Sometimes new technology can fit into existing doctrine.[156] But new

---

www.softwareadvice.com/security/industryview/right-to-be-forgotten-2014/ [https://perma.cc/U6JQ-C8PV].

[151] Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RES. CTR. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/ [https://perma.cc/8M8W-359T].

[152] *Id.*

[153] *See* Pern Hui Chia, Yusuke Yamamoto & N. Asokan, *Is This App Safe?: A Large Scale Study on Application Permissions and Risk Signals*, Proceedings of the 21st Int'l Conference on World Wide Web 311 Apr. 16–20, 2012, Lyon, France [doi> 10.1145|2187836.2187879].

[154] *See* Joshua Fogel & Elham Nehmad, *Internet Social Network Communities: Risk Taking, Trust, and Privacy Concerns*, 25 COMPUTERS IN HUM. BEHAV. 153 (2009). For a technocratic legal approach to Internet of Things privacy issues see Rolf H. Weber, *Internet of Things: Privacy Issues Revisited*, 31 COMPUTER L. & SECURITY REV. 618 (2015).

[155] *See* Ruogu Kang et al., *"My Data Just Goes Everywhere": User Mental Models of the Internet and Implications for Privacy and Security*, 2015 SYMPOSIUM ON USABLE PRIVACY & SECURITY 39 (2015). The study found that users who have more technical knowledge of the internet tend to understand privacy risks better than laypeople. *Id.* at 43–46.

[156] For an example of explicit judicial pushback on the idea that technology should specifically affect the law, see Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. L. FORUM 207 (1996) (considering "cyberspace law" to be "multidisciplinary dilettantism" and suggesting lawyers and judges simply apply existing sound legal principles to new technology).

technology inevitably exerts pressure on the law.[157] Whether the Justices admit it or not, the Court has a long history of revisiting, refining, and (occasionally) reversing itself in response to changing technosocial realities.[158]

Every so often, the Court will openly concede that then-existing doctrine is not equipped to handle modern circumstances, precipitating a legal paradigm shift.[159] Whether slow or rapid, many areas of the law have proven susceptible to changes in technology available to the public or to the government. For instance, famously, the Court was compelled in 1945 to scrap and reform its personal jurisdiction framework.[160] As any first-year law student knows, in its 1878 holding in *Pennoyer v. Neff*,[161] the Court articulated its view of a sovereign's personal jurisdiction over a defendant.[162] The nineteenth-century *Pennoyer* view was that courts of law or equity, in accordance with the Due Process clause,[163] could only exercise jurisdiction over persons or property *actually present* within the jurisdiction's sovereign territory, or over persons who otherwise *consented*.[164] This formalistic concept of sovereign jurisdiction befitted a horse-and-buggy age where wire communication was limited.[165]

---

[157] *See, e.g.*, Circuit City Stores, Inc. v. CarMax, Inc., 165 F.3d 1047, 1057 (6th Cir. 1999) (Jones, J., concurring) (suggesting in light of technological change that courts reconsider doctrine of the geographic scope of trademark rights) ("[G]iven that recent technological innovations such as the Internet are increasingly deconstructing geographical barriers for marketing purposes, it appears to me that a reexamination of precedents would be timely.").

[158] *But see* Brown v. Entm't Merchs. Ass'n, 564 U.S. 786 (2011) (holding video games sales to minors are protected under First Amendment principles, and invalidating a content-based ratings system for video games). Justice Scalia wrote for the majority in *Entertainment Merchants*, but note that Scalia joined the dissent in *Bartnicki*. Bartnicki v. Vopper, 532 U.S. 514, 541 (2001) (Rehnquist, C.J., dissenting). For more on *Entertainment Merchants*, see *infra* Part IV.

[159] *See generally* THOMAS KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (1st ed. 1962) (proposing a now famous theoretical model for widespread adoption of new ideas, for example the heliocentric model of our solar system).

[160] *See* International Shoe Co. v. Washington, 326 U.S. 310 (1945) (introducing the idea of personal jurisdiction based on "minimum contacts").

[161] 95 U.S. 714 (1878).

[162] *Id.* at 727 ("Process from the tribunals of one State cannot run into another State, and summon parties there domiciled to leave its territory and respond to proceedings against them.").

[163] U.S. CONST. amend XIV, § 1 ("[N]or shall any state deprive any person of life, liberty, or property, without due process of law . . . .").

[164] *Pennoyer*, 95 U.S. at 729 (mentioning "voluntary appearance" as allowing valid exercise of personal jurisdiction).

[165] The earliest electrical telegraphy communications systems were implemented in 1837 in England. *See* LEWIS COE, THE TELEGRAPH: A HISTORY OF MORSE'S INVENTION AND ITS PREDECESSORS IN THE UNITED STATES 15 (1993). By the time *Pennoyer* was decided in 1878, there were several transatlantic telegraph lines in operation and some transcontinental ones too. However, the American west was substantially unconnected. *See* G.W. & C.B. Colton & Co., Map Showing the Telegraph Lines In Operation, Under Contract, and Contemplated to Complete the Circuit of the Globe (c. 1870–71), LIBRARY OF CONGRESS, http://hdl.loc.gov/loc.gmd/g3201p.ct001637 [https://perma.cc/M56S-Q43V] (last visted Oct. 15, 2018).

The *Pennoyer* decision barely postdated the first telephone,[166] and long predated the radio,[167] and the automobile.[168]

Over successive decades, with the advent of new communications technology, massive multistate and multinational corporations, and rapid transit, it became fundamentally impracticable to adhere to the formalism of *Pennoyer*. With increased mobility of persons and goods, the Court strained itself to expand principles of consent to the point approaching absurdity and stretch other legal mechanisms such as *quasi-in-rem* jurisdiction.[169]

Finally, in 1945 the realities of the day compelled the Court to discard its formalist framework. In *International Shoe Co. v. Washington*,[170] the Court set up a functionalist framework based on a party's "certain minimum contacts" with the forum territory.[171] Subsequent developments in personal jurisdiction doctrine have relied on abstract concepts such as "stream of commerce" suited to the present day.[172]

The Court had no choice but to adjust its views on personal jurisdiction as technology caused changes in society. Recently, courts have struggled with the notions of venue and personal jurisdiction in matters of wrongdoing in cyberspace.[173] Courts

---

[166] *See* Joan Brodsky Schur, *Telephone & Light Patent Drawings*, U.S. NAT'L ARCHIVES, https://www.archives.gov/education/lessons/telephone-light-patents [https://perma.cc/VR73-AVQ6] (last updated Sept. 7, 2016); *see also* U.S. Patent. No. 174,465 (issued Mar. 7,1876).

[167] *See* Prabir K. Bondyopadhyay, *Guglielmo Marconi—The Father of Long Distance Radio Communication: An Engineer's Tribute*, 25th European Microwave Conference Sept. 4, 1995, Bologna, Italy [doi: 10.1109|EUMA.1995.337090]. Marconi invented the first radio communications apparatus around 1900.

[168] The first commercially available internal-combustion automobiles appeared in the mid-1890s. *See Company History*: *Benz Patent Motor Car: The First Automobile (1885–1886)* DAIMLER, https://www.daimler.com/company/tradition/company-history/1885-1886.html [https://perma.cc/U6E2-ZDHV] (last visited Oct. 15, 2018). Ford Motor Co. sold its first commercial automobile in 1903, and first sold its famed Model T in 1908. *See Our History,* FORD MOTOR CO., https://corporate.ford.com/history.html [https://perma.cc/HV4N-S7EP] (last visited Oct. 15, 2018).

[169] *See, e.g.*, Hess v. Pawloski, 274 U.S. 352, 356 (1927) (driving a motor vehicle into Massachusetts sufficient to consent to personal jurisdiction and appointment of agent for service of process); *see also* Henry L. Doherty & Co. v. Goodman, 294 U.S. 623, 627–28 (1935) (upholding personal jurisdiction over company whose agents were selling securities in forum state); Harris v. Balk, 198 U.S. 215 (1905) (a court can assume *quasi-in-rem* jurisdiction over a defendant wherever her debtors can be found).

[170] 326 U.S. 310 (1945).

[171] *Id.* at 316 (quoting Milliken v. Meyer, 311 U.S. 457, 463 (1940)).

[172] *See* J. McIntyre Machinery v. Nicastro, 564 U.S. 873, 879 (2011); Asahi Metal Indus. Co. v. Superior Court, 480 U.S. 102, 105 (1987); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286 (1980); *see also* Hanson v. Denckla, 357 U.S. 235 (1958) (providing a good overview of *in rem* jurisdiction and personal jurisdiction).

[173] *See, e.g.*, Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisémitisme, 433 F.3d 1199 (9th Cir. 2006) (confirming that the district court did have personal jurisdiction, although a close call, over French association (LICRA), but due to ripeness concerns, decision in favor of

have generally refused to permit the physical location of servers to shield United States–based actors from liability.[174] However, in February 2018, the Supreme Court heard argument in *Microsoft Corp. v. United States*,[175] a case that again forced it to confront the realities of the twenty-first century. There, the petitioners asked the Court to address whether the federal government can, through a lawful request, exercise control over data held on a server not located in United States territory.[176] About a month after oral argument, Congress passed the CLOUD Act, clarifying the issue and mooting the case.[177] Still, *Microsoft* illustrates how courts have and will continue to confront technological shifts that are poorly suited to existing law. Whether through the courts or legislature, the law must adjust.

Yahoo! was reversed and case remanded to the district court to dismiss without prejudice). In principle, the Ninth Circuit agreed with the district court's refusal to enforce a French judgment in California for the online auction of Nazi memorabilia which, under French Law, was illegal. *See id. See also* United States v. Drew, 259 F.R.D 449 (C.D. Cal. 2009) (charging defendant with violations of the Computer Fraud and Abuse Act in the Central District of California, although both defendant and victim were residents of Missouri, because the allegedly violative communications passed through servers physically located in California). For a discussion on jurisdictional issues relating to web-based activity, see Teresa Scassa & Robert J. Currie, *New First Principles? Assessing the Internet's Challenges to Jurisdiction*, 42 GEO. J. INT'L L. 1017 (2011).

[174] For examples of cases where courts have found jurisdiction over servers hosting illegal gambling activity, see *United States v. America Sports Ltd.*, 286 F.3d 641 (3d Cir. 2002); *United States v. Ross*, No. 98 CR. 1174-1(KMV), 1999 WL 782749, at *1 (S.D.N.Y. Sept. 16, 1999); *People v. World Interactive Gaming Corp.*, 714 N.Y.S.2d 844 (Sup. Ct. 1999).

[175] 138 S. Ct. 1186 (2018).

[176] The question that confronted the Supreme Court in *Microsoft* was whether a corporation must comply with a government request under the Stored Communications Act by disclosing electronic communications within that corporation's control, even if the electronic data is stored on server geographically outside the United States. *See In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), *cert. granted*, United States v. Microsoft Corp., 136 S. Ct. 356 (2017). The case was ultimately mooted by an act of Congress. *See* United States v. Microsoft, 138 S. Ct. 1186 (2018); *see also infra* note 177. While the legal issue in this case was jurisdictional, the factual predicate the Court was asked to weigh in on was novel technology. *See also* Transcript of Oral Argument at 6, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2) ("I think the starting point, all would agree, in . . . 1986, no one ever heard of clouds. This kind of storage didn't exist."); Amy Howe, *Argument Preview: Old Laws, New Technology and National Borders*, SCOTUSBLOG (Feb. 21, 2018, 10:45 AM), http://www.scotusblog.com/2018/02/argument-preview-old-laws-new-technology-national-borders/ [https://perma.cc/7DQZ-BLS4] ("In 1986, when Congress passed the Stored Communications Act, the World Wide Web did not yet exist . . . the justices will consider a question that Congress likely didn't think about 32 years ago."); Steve Nickelsburg et al., *Overseas Data Seizures—U.S. Supreme Court Hears Oral Argument, But Congress Might Get to the Issue First*, CLIFFORD CHANCE (Mar. 2018), https://www.cliffordchance.com/briefings/2018/03/overseas_data_seizuresussupremecourthear.html [https://perma.cc/EM25-92C5].

[177] Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 4943, 115th Cong. (2018) (enacted).

Technosocial change has perhaps impacted no area of constitutional jurisprudence more than the Fourth Amendment search and seizure doctrine.[178] Early developments in Fourth Amendment jurisprudence were rooted in property law, interpreting a search or seizure as akin to a common-law trespass on property.[179] In 1928, in *Olmstead v. United States*,[180] a divided Court held a wiretap of a public phone not to be a search or seizure within the meaning of the Fourth Amendment because there was not a trespass on private property.[181] In dissent, Justice Brandeis gave eloquent voice to the specific proposition that technology must inevitably shape constitutional law:

> Since [*McCulloch v. Maryland*][182] this [C]ourt has repeatedly sustained the exercise of power by Congress, under various clauses of [the Constitution], over objects of which the fathers could not have dreamed . . . . Clauses guaranteeing to the individual protection against specific abuses of power must have a . . . capacity of adaptation to a changing world.[183]

---

[178] *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33–34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."); City of Ontario v. Quon, 560 U.S. 746, 759 (2010) ("Rapid changes in the dynamics of communication and information transmission are evident not just in technology itself but in what society accepts as proper behavior."). For perspectives on the impact of technology on Fourth Amendment jurisprudence see Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614 (2011) (arguing Fourth Amendment protections are impossible to disentangle from technological and social factors and should extend beyond the physical home to a citizen's online presence); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (arguing that legislatures are better equipped than courts to adjust constitutional principles to emerging technologies); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086 (2002) (arguing that Fourth Amendment doctrine does not protect privacy sufficiently against new technologies, and that Fourth Amendment law should create an "architecture of power" to maintain an appropriate balance of power among individuals, institutions, and the government in light of "the ever-increasing data flows of the Information Age"). For an overview of search and seizure doctrine in the early twentieth century, see Hugh E. Willis, *Unreasonable Searches and Seizures*, 4 IND. L. J. 311 (1928).

[179] *See* Solove, *supra* note 178, at 1122 ("The Court originally conceptualized privacy in physical terms as protecting tangible property or preventing trespasses.") (internal citations omitted).

[180] 277 U.S. 438 (1928).

[181] *Id.* at 464–65 ("There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants . . . [T]he language of the [Fourth] Amendment can not be extended and expanded to include telephone wires . . . .").

[182] 17 U.S. (4. Wheat.) 316, 407 (1819) ("[W]e must never forget, that it is a *constitution* we are expounding.").

[183] *Olmstead*, 277 U.S. at 472 (Brandeis, J., dissenting) (internal citations omitted).

In 1967, as Justice Brandeis foreshadowed, the Court reversed *Olmstead* in *Katz v. United States*, holding that a warrantless wiretap of a phone booth violated Fourth Amendment guarantees.[184] Justice Stewart, writing for the majority, eschewed rote principles of trespass on property.[185] Declaring "the Fourth Amendment protects people, not places,"[186] *Katz* set forth what later courts adopted as the now-famous "reasonable expectation of privacy" test.[187]

In principle, the *Katz* reasonable expectation of privacy test applies to emerging technologies as societal expectations develop.[188] But the Court has been repeatedly tested in applying Fourth Amendment doctrine to emerging technologies. The Court has churned out a casebook-worth of doctrine relating to warrantless searches of automobiles.[189] In 1984, the Court held that certain chemical tests used to detect cocaine do not require a warrant.[190] In 2001, the Court held that warrantless use of a thermal imaging camera to view the inside of a home violates the Fourth Amendment.[191]

In *United States v. Jones*,[192] the Court held that warrantless use of a GPS tracking device is violative of the Fourth Amendment.[193] In an opinion by Justice Scalia, the

---

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

[185] *Id.* at 351 ("[T]he parties have attached great significance to the characterization of the telephone booth from which the petitioner placed his calls . . . . But this effort to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem in this case.").

[186] *Id.*

[187] *Id.* at 360–61 (Harlan, J., concurring in the judgment).

[188] *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2495 (2014) (holding officers may not search information on a cell phone without a warrant):

> Absent more precise guidance from the founding era, we generally determine whether to exempt a given type of search from the warrant requirement by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.

Id. at 2484 (internal quotations omitted).

[189] *See* Arizona v. Gant, 556 U.S. 332 (2009) (holding an officer may search vehicle passenger compartment without a warrant when the officer has a reasonable suspicion that an individual, whether an arrestee or not, is dangerous and might access the vehicle to gain control of a dangerous weapon); Thornton v. United States, 541 U.S. 615 (2004) (holding an officer may lawfully search an arrestee's passenger compartment without a warrant as a contemporaneous incident to arrest, even if the officer makes contact with the arrestee outside the vehicle); New York v. Belton, 453 U.S. 454 (1981) (holding an officer may lawfully search an arrestee's passenger compartment, and closed containers found within the passenger compartment, without a warrant as a contemporaneous incident to arrest); *see also* New York v. Class, 475 U.S. 106 (1986); Michigan v. Long, 463 U.S. 1032 (1983); United States v. Ross, 456 U.S. 798 (1982); Carroll v. United States, 267 U.S. 132 (1925).

[190] United States v. Jacobsen, 466 U.S. 109, 125 (1984).

[191] Kyllo v. United States, 533 U.S. 27, 40 (2001). In *Kyllo*, Justice Scalia considered the Court's role not as adapting to new technologies but rather preserving the privacy that citizens relied upon in the past. *See id.* at 34.

[192] 565 U.S. 400, 404 (2012).

[193] *Id.*

Court held the attachment of a GPS device to one's vehicle constituted a common-law trespass.[194] Concurring in the judgment, Justice Sotomayor explicitly pointed to new technology as vexing contemporary Fourth Amendment jurisprudence.[195] She suggested that government monitoring of GPS-enabled smartphones and other modes of electronic surveillance that do not involve physical trespass must be approached through evolving societal expectations under the lens of the *Katz* test.[196]

In June 2018, a sharply divided Court decided in *Carpenter v. United States*[197] that days' worth of an individual's physical movements, as captured by cell-site location information (i.e., time-stamped records of locations where a cellular phone connects to a signal tower), is protected under the Fourth Amendment, and therefore to obtain such records the government generally must obtain a search warrant supported by probable cause.[198] Previously, the Court had held that the inspection of personal records held by third parties, such as billing information or call logs, was not a "search" within the meaning of the Fourth Amendment.[199] Chief Justice Roberts, writing for the majority, pointed directly at technosocial change in his reasoning: "[I]n 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." The Court concluded that, although "[t]his sort of digital data . . . does not fit neatly under existing precedent,"[200] individuals have a reasonable expectation of privacy in such information; therefore it is protected under the Fourth Amendment.[201] The law once again yielded to technosocial change as the Court confronted the reality that servers now hold as much or more sensitive information than our bedside drawers.

The Court, however, likes to insist its principles are unwavering. In *Brown v. Entertainment Merchants Association*, for instance, the Court found that videogames qualify for free speech protections, holding unconstitutional a California law prohibiting sale to minors of certain games depicting "killing, maiming, dismembering, or sexually assaulting an image of a human being," and requiring such games to be specially labeled.[202] In *Entertainment Merchants*, Justice Scalia asserted "whatever the challenges of applying the Constitution to ever-advancing technology, the basic

---

[194] *Id.* at 406–10.

[195] *Id.* at 418 (Sotomayor, J., concurring).

[196] *Id.* at 415.

[197] 138 S. Ct. 2206 (2018).

[198] *Id.* At oral argument, counsel for Carpenter argued: "We are well over two decades into the cell phone age. This is an area where . . . people's use of this technology is well-settled and only becoming more pervasive over time. We know the . . . direction, the cases before the Court now, and . . . it is crucial that the Court act." Transcript of Oral Argument at 78, United States v. Carpenter, 138 S. Ct. 2206 (2018) (No. 16-402).

[199] *See* Smith v. Maryland, 442 U.S. 735, 744–46 (1979).

[200] *Carpenter*, 138 S. Ct. at 2214.

[201] *See id.* at 2217–19.

[202] 564 U.S. 786, 789 (2011). *See also* CAL. CIV. CODE §§ 1746–1746.5 (West 2009).

principles of freedom of speech and the press . . . do not vary when a new and different medium for communication appears."[203] The issue with *Bartnicki*, though, is not about new technology, *per se*, but about the massive proliferation of a volume and range of technologies that reshape society.[204]

And whether the Court admits or not, the Court has decided that changes in technology warrant serious consideration and reconsideration of constitutional interpretation and application.[205] In this instance, rapid shifts in technology and overwhelming risks to information privacy merit revisiting *Bartnicki*.

IV. THE MASSIVE TECHNOSOCIAL CHANGE SINCE 2001 SPECIFICALLY WARRANTS REVISITING *BARTNICKI*

As the above Sections make clear, (1) since 2001, information technology has grown dramatically and reshaped American society; (2) privacy interests are now at far greater risk than they were in 2001; and (3) the Supreme Court has a history of shaping its doctrine in accord with technosocial changes in society at large. Following these precepts, the holding in *Bartnicki* should be relaxed to offer law-makers wider latitude in protecting information privacy.

A. The Government Already Imposes Lawful Restrictions on Certain Disclosures of Truthful Information

In his majority opinion in *Bartnicki*, Justice Stevens, glossing over privacy as a compelling interest, makes a curious remark. In an attempt to narrow the scope of his holding, he notes that the Court refuses "to answer categorically whether the publication of truthful information may ever be punished consistent with the First Amendment."[206] The remark is curious because, as Justice Breyer points out in his concurrence,[207] this supposedly open question has clearly been answered in the affirmative. Certain truthful information may be prohibited from publication, and its publication may be punished consistent with the First Amendment.

---

[203] *Entm't Merchs. Ass'n*, 564 U.S. at 790 (internal quotation marks omitted). The Court understood the apparent oddity of applying originalist principles to videogames. At oral argument, Justice Alito quipped, "I think what Justice Scalia wants to know is what James Madison thought about video games. . . . Did he enjoy them?" Transcript of Oral Argument at 16, Schwarzenegger v. Entm't Merchs. Ass'n, 564 U.S. 786 (2011) (No. 08-1448).

[204] Recall that Justice Scalia dissented in *Bartnicki*.

[205] *But see generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (arguing, *inter alia*, that legislatures are better equipped than courts to adjust constitutional principles to emerging technologies).

[206] Bartnicki v. Vopper, 532 U.S. 514, 529 (2001).

[207] *Id.* at 539 (Breyer, J., concurring).

The law, and the Supreme Court, have long recognized communications privacy and promotion of private speech as a compelling government interest; the Court likewise has recognized personal privacy as an interest protected under the Constitution.[208] For example, as Justice Breyer cites, the publication of a trade secret is punishable by money damages or an injunction, depending on the circumstances.[209] A trade secret is said to be destroyed by public knowledge,[210] and thus public disclosure may be interdicted—actual or threatened misappropriation of a trade secret (e.g., the Coca-Cola syrup recipe) may be enjoined although even though truthful and of public concern.[211]

Although First Amendment principles generally limit *prior restraint* on public disclosure, such as injunctions, courts are willing to impose damages under certain circumstances.[212] Lately developed common law recognizes public disclosure of objectionable private information as a tort of "invasion of privacy" in some circumstances.[213] The common law also imposes certain duties of confidentiality and discretion on fiduciaries, such as trustees and lawyers, breaches of which are recoverable for damages in litigation.[214] Courts consistently enforce private non-disclosure agreements, even if the confidential information may touch on matters of public concern.[215]

Furthermore, Congress has repeatedly taken steps to protect certain private information and has created statutory penalties for unlawful breach and dissemination.

---

[208] *See* Roe v. Wade, 410 U.S. 113, 152 (1973) ("In a line of decisions . . . the Court has recognized that a right of personal privacy . . . does exist under the Constitution."); Katz v. United States, 389 U.S. 347, 353 (1967); *see also* Griswold v. Connecticut, 381 U.S. 479, 483 (1965) ("[T]he First Amendment has a penumbra where privacy is protected from governmental intrusion.").

[209] *See Bartnicki*, 532 U.S. at 539 (Breyer, J., concurring) (citing Restatement (Third) of Unfair Competition § 40, Comment c (1995)); *see also, e.g.*, Winston Research Corp. v. Minn. Min. & Mfg. Co., 350 F.2d 134 (9th Cir. 1965) (affirming a two-year injunction on sales of tape recorder device that was designed and manufactured using misappropriated trade secret knowledge); Ferdinand S. Tino, Annotation, *Propriety of permanently enjoining one guilty of unauthorized use of trade secret from engaging in sale or manufacturing of device in question*, 38 A.L.R. 3d 572, § 5a (1971); 42 Am. Jur. 2d *Injunctions* § 132 (2018) (owner of a trade secret may obtain injunction against use or disclosure by another).

[210] *See* UNIF. TRADE SECRETS ACT (UNIF. LAW COMM'N 1985).

[211] *Id.* § 2 ("Actual or threatened misappropriation may be enjoined.").

[212] *See, e.g.*, Near v. Minnesota, 283 U.S. 697 (1931).

[213] *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977).

[214] *See* RESTATEMENT (SECOND) OF AGENCY, §§ 395–96 (AM. LAW INST. 1958) (concerning use and disclosure of confidential information by fiduciaries); RESTATEMENT (THIRD) OF UNFAIR COMPETITION, §§ 39–45 (AM. LAW INST. 1995) (paralleling RESTATEMENT (FIRST) OF TORTS, §§ 757–59 (AM. LAW INST. 1939)) (concerning liability for divulging trade secrets); RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS §§ 59–67 (AM. LAW INST. 2000) (concerning a lawyer's duty of confidentiality).

[215] California has passed statutes limiting confidentiality of settlement agreements in cases where the factual foundation for the settlement represents the cause of action for certain sexual offenses. *See, e.g.*, 2016 CAL. STAT. 876 (amending CAL. CIV. PROC. CODE § 1002). *See also* Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261 (1998).

These include the Federal Rules of Criminal Procedure,[216] the Federal Rules of Civil Procedure,[217] the Espionage Act,[218] the Privacy Act,[219] the Intelligence Identities Protection Act,[220] the Fair Credit Reporting Act,[221] the Electronic Communications Privacy Act,[222] the Video Privacy Protection Act,[223] the Cable Television Consumer Protection and Competition Act,[224] the Health Insurance Portability and Accountability Act (HIPAA),[225] the Children's Online Privacy Protection Act (COPPA),[226] and the Wiretap Act itself,[227] among numerous others. Each of these statutes carves out various duties of reporting and confidentiality and penalties for breach of such provisions.

These legal principles and statutes demonstrate various ways where courts and legislators have attempted to tailor the law to prioritize and protect privacy interests in specific circumstances.

---

[216] *See* FED. R. CRIM. P. 6(e)(2)(B) (imposing secrecy obligation on certain persons involved in a grand jury proceeding).

[217] *See* FED. R. CIV. P. 26(c) (detailing rules for various protective orders, including secrecy, in discovery). Also consider the rules of ethics for practicing attorneys, and expectations of confidentiality. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT 1.6 (AM. BAR. ASS'N 1983).

[218] Espionage Act of 1917, Pub. L. 65-24, 40 Stat. 217 (codified as amended at 18 U.S.C. §§ 792–99 (2012)).

[219] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552a (2012)) (amending the Administrative Procedure Act to require federal agencies to maintain minimum privacy and disclosure standards).

[220] Intelligence Identities Protection Act, Pub. L. No. 97-200, 96 Stat. 122 (codified as amended at 50 U.S.C. §§ 421–26 (2012)).

[221] Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1830–31, 15 U.S.C. §§ 1681–81x (2012)) (amending the Federal Deposit Insurance Act to require ensured financial institutions to maintain records and privacy procedures).

[222] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (extending protections of Wiretap Act to include electronic communications such as email, and extending protections to stored electronic files and phone call tracing technologies) (codified as amended at 18 U.S.C. §§ 2510–20, 2701–12, 3121–27 (2012)).

[223] Video Game Privacy Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (creating a private cause of action against a covered entity who reveals customer's video rental history) (codified as amended at 18 U.S.C. § 2710 (2012)).

[224] Cable Television Consumer Protection and Competition Act of 1992, Pub. L. No. 102 -385, 106 Stat. 1460 (establishing numerous rules and regulations for subscription television services, including subscriber privacy rules) (codified as amended at 47 U.S.C. § 551 (2012)).

[225] Health Insurance and Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 The patient privacy provisions are codified at 42 U.S.C. §§ 1302(a), 1320d to 1320d-9. *See also* 45 C.F.R. §§ 160.101 to 160.552, 164.102 to 164.106; 164.500 to 164.534.

[226] Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 -728 (creating minimum consent, confidentiality, and disclosure for personally identifying information of persons under 13 years of age) (codified at 15 U.S.C. §§ 6501–06 (2012)).

[227] Pub. L. 90-351, 82 Stat. 197 (1968); 18 U.S.C. §§ 2510–22.

B. The Law Can Protect Communication Privacy Interests in Certain Limited Ways, Without Unduly Burdening Free Speech

The theft of information such as from a server or phone conversation is reminiscent of situations lately implicating the Fourth Amendment's "reasonable expectation of privacy standard."[228] Fourth Amendment principles lend themselves, by analogy, reasonably well to the *Bartnicki* context. The balance of Free Speech interests should be judged against the privacy interests of the communicant, including her reasonable expectation of privacy. Where the interests of the publisher are merely salacious or prurient, as in publication of stolen private sexual material, even prior restraint of speech may be warranted.

The statute at issue in *Bartnicki* already narrowed that category of punishable conduct to publication where the publisher "*knew or should have known*" the information had been obtained illegally.[229] In other words, the publishing party is not utterly blameless, but is simply placed in the role of discriminating against wrongdoers. It is true that Justice Stevens confined his holding by centering his reasoning on the *content* of the stolen information, through the "amorphous concept"[230] of "public concern," meaning so long as the leaked material is salacious enough to the public, it is unprotected for First Amendment privacy interest purposes.

The Supreme Court has long applied a "public concern" heuristic in Free Speech cases,[231] in particular those involving either government employees or defamation.[232] In the government employment context, a government employee may be punished for public statements unless the statements touch on matters of public concern, after which a balancing test is applied, weighing the interests of the government body against the free speech interests of the employee.[233] In this case, though, "public concern" operates as against the public at large, and squares with the Court's long-time, understandable

---

[228] *See generally* Katz v. United States, 389 U.S. 347 (1967) (holding that a speaker has a reasonable expectation of privacy over a conversation in a sealed phone booth).

[229] 18 U.S.C. § 2511(1)(c) (emphasis added).

[230] *See* Bartnicki v. Vopper, 532 U.S. 514, 542 (2001) (Rehnquist, C.J., dissenting).

[231] *See* Connick v. Myers, 461 U.S. 138 (1983) (holding that a public employee's free speech rights depend in part on whether the employee's speech touches on matters of public concern); Pickering v. Bd. of Educ., 391 U.S. 563 (1968) (holding that public employees may not be compelled to relinquish Free Speech rights to comment on matters of public concern); *cf.* Garcetti v. Ceballos, 547 U.S. 410 (2006) (holding that when public employees make statements pursuant to their own official duties, they are not speaking as citizens on matters of public concern for First Amendment purposes).

[232] *See* Gertz v. Robert Welch, Inc., 418 U.S. 323 (1974) (restricting damages a private individual could obtain from a publisher in defamation cases where the subject matter at issue was of public concern); Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 760–61 (1985) (delineating a "reduced constitutional value of speech involving no matters of public concern" when calculating damages in defamation cases).

[233] *See supra* note 231.

reluctance to punish publication on matters that touch on public policy, such as the Pentagon Papers.[234]

The "amorphous" public concern test is in practice unwieldy. Matters *possibly* or *arguably* of public concern, such as corporate communications, are extremely vulnerable to theft and disclosure.[235] Consider the stolen batch of emails of Clinton campaign chairman John Podesta that contained numerous communications about campaign strategy and policy—arguably matters of public concern, but also important private, internal campaign communication, the likes of which is probably chilled in future national-office campaign efforts.[236] Additionally, the batch of Podesta emails contained numerous private exchanges, recipes, and information about children,[237] all potentially protected under *Bartnicki* as matters of public concern. Is a court to review each of the 20,000 emails and decide which are and are not of public concern?

Drawing from the example of the State of Washington's wiretap statute, which carves out disclosure exceptions in certain emergencies,[238] I would suggest a narrower definition of "public concern." It is a matter of "public concern" when it implicates a credible and substantial safety threat against the public, a specific group, or a

---

[234] The "newsworthiness" certainly seems relevant. It is not ridiculous to suppose *Bartnicki* was an example of easy facts making bad law. The transcript of Bartnicki and Kane's recorded conversation seems as though two high-ranking union officials were planning acts of violence against local government employees. It would be difficult for the Court to allow the punishment of a newspaper for sharing that information with the public.

[235] *See* discussion *supra* Part II.

[236] *See* Matthew Yglesias, *Against Transparency*, VOX (Sept. 6, 2016), https://www.vox.com/2016/9/6/12732252/against-transparency [https://perma.cc/9Y55-MBXP] (arguing executive branch officials' electronic communications should be confidential to promote candor and efficiency) ("[A] private conversation to facilitate a frank exchange of ideas is not the same as a secret bombing campaign in Cambodia. We need to let public officials talk to each other—and to their professional contacts outside the government—in ways that are both honest and technologically modern.").

[237] *See, e.g.*, Lawrence Marcus, *Wikileaks Hack Reveals John Podesta's Secret to Creamy Risotto*, FOOD & WINE (Oct. 11, 2016), https://www.foodandwine.com/news/wikileaks-hack-reveals-john-podestas-secret-creamy-risotto [https://perma.cc/VN6K-A2S3]. For other examples of stolen emails that would probably not meet a reasonable definition of "public concern," see *It's a Girl!*, WIKILEAKS: ARCHIVE OF JOHN PODESTA EMAILS, https://wikileaks.org/podesta-emails/emailid/47663 [https://perma.cc/5SKY-YX5M] (last visited Oct. 15, 2018) (announcing the birth of a healthy baby girl); *Re: Connecting*, WIKILEAKS: ARCHIVE OF JOHN PODESTA EMAILS, https://wikileaks.org/podesta-emails/emailid/40914 [https://perma.cc/A88C-TEU5] (last visited Oct. 15, 2018) (describing plans to attend a meeting of a book club); *Re: Nicki Minaj Doesn't Think Her Butt Is Unacceptable | ThinkProgress*, WIKILEAKS: ARCHIVE OF JOHN PODESTA EMAILS, https://wikileaks.org/podesta-emails/emailid/18048 [https://perma.cc/8V6Y-TLUE] (last visited Oct. 15, 2018) (Podesta remarking on "booty equity").

[238] *See* WASH. REV. CODE §§ 9.73.030(2), (4) (2018) (deeming consent of a party where intercepted conservation relates to certain emergency situations); *see also Bartnicki*, 532 U.S. 514, 539 (Breyer, J., concurring) ("Where publication of private information constitutes a wrongful act, the law recognizes a privilege allowing the reporting of threats to public safety.").

specific individual. This would create a clearer rule, which protects the interests of publishers of information regarding threats to public safety and which is consistent with sound public policy observed in other areas of the law.[239] Congress could also authorize the Federal Communications Commission (FCC) to define what are matters of public concern, much as the FCC already defines what is profane.

The Court, too, could draw boundaries that would offer more certainty and a broader range of applications for punishing the dissemination of stolen conversations and personal information. For instance, certain contours of public concern as applied to this statute could be left to the jury.

And as both the Court of Appeals and the dissent point out in Bartnicki, § 2511 of the Wiretap Act—the section at issue in the case—was content-neutral,[240] and therefore was not subject to strict scrutiny, theoretically leaving some judicial room for legislative tinkering. The Wiretap Act exists to protect and ensure the privacy of one's home, which is recognized as an important constitutional interest.[241] Justice Brandeis understood the great importance of privacy interests back in the nineteenth century.[242] An unambiguous privacy safeguard written in the law reassures individuals to "overcome our natural reluctance to discuss private matter when we fear that our private conversations may become public."[243] Seen through this lens, the initial misappropriation of private information is not the harmful activity so much as the mass disclosure to the community—after all, the petitioners in *Bartnicki* were concerned not so much with the interception of their conversation but with the broadcast. Furthermore, as Justice Stevens admits in *Bartnicki*, the anti-wiretap statute already restricts the free speech interests of the thief herself, and Stevens is not willing to hold that the thief cannot be punished under § 2511(1)(c).

---

[239] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 595 cmt. g (AM LAW INST. 1977) (privilege to report that another intends to kill or rob); *id.* § 652G (privilege applies as a defense to invasion of privacy); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. c (AM. LAW. INST. 1995) (trade secret may be disclosed if relevant to public health or safety); MODEL R. PROF'L CONDUCT 1.6(b)-(1) (AM. BAR. ASS'N 1983) (lawyer-client confidentiality may be broken where there is a risk of severe injury or death of another); *see also* Lachman v. Sperry-Sun Well Surveying Co., 457 F.2d 850, 852 (10th Cir. 1972) (non-disclosure agreement void as to criminal activity); Tarasoff v. Regents of Univ. Cal., 551 P.2d 334, 343–44 (Cal. 1976) (psychologist-patient privilege not binding where there is a specific danger to another).

[240] *See Bartnicki*, 532 U.S. at 548 (Rehnquist, C.J., dissenting).

[241] *See, e.g.*, Roe v. Wade, 410 U.S. 113, 152 (1973) ("In a line of decisions . . . the Court has recognized a right of personal privacy . . . does exist under the Constitution."); Griswold v. Connecticut, 381 U.S. 479, 483 (1965) ("[T]he First Amendment has a penumbra where privacy is protected from governmental intrusion.").

[242] *See* Pavesich v. New Eng. Life Ins., Co., 50 S.E. 68 (Ga. 1905). *See generally* Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (articulating various features in the law collectively giving rise to a "right to be left alone").

[243] *Bartnicki*, 532 U.S. at 537.

Finally, as jurisprudential deference goes, it is important to note the majority in *Bartnicki* was a "soft" majority. Three justices agreed with Justice Stevens, and two joined the judgment in concurrence. But looking at the opinions another way, a five-justice majority agreed that Congress could constitutionally punish certain third-party publications. The soft majority in the original decision suggests there is significant disagreement on the Court over this issue. The Court should not feel constrained in revisiting the issue, and the dissent has already previewed the grounds for reversal.

CONCLUSION

Bartnicki exists in a nebula of numerous forces that are chilling private speech. Savvy tech users are resorting to high-end encryption technologies. Corporations are adopting strict, onerous communications policies to avoid misappropriation of communications. A reversal or relaxation of *Bartnicki* would offer an important tool to those who have been victimized by near-ubiquitous eavesdropping and information theft and would create a small, but meaningful deterrent against those who might engage in such behavior.

A *complete* reversal of *Bartnicki* is not necessary nor desirable. The Free Speech interests at its heart are of grave importance. But there are several aspects of *Bartnicki* that could be tailored. A balanced principle more consistent with Justice Breyer's concurrence would be desirable. Specifically, the legitimacy of a would-be-plaintiff's privacy interest, including her reasonable expectations of privacy under the circumstances, should be weighed against the First Amendment interests at issue.

Additionally, *Bartnicki*'s crucial "public concern" element is problematic in this context because (1) it is subjective; (2) it imposes a post facto content-based test after the theft and transfer of information we want to deter; and (3) leaks may be of "mixed composition" where they could be of limited or partial public concern. Legislatures could therefore attempt to legislate a suitable definition of "public concern" or delegate authority to an agency to do so. Regardless what the specific prescription is, "the Constitution permits legislatures to respond flexibly to the challenges future technology may pose . . . ."[244]

Setting *Bartnicki* itself aside, Congress and the courts will inevitably face the tide of technosocial change. In his *Olmstead* dissent, Justice Brandeis hypothesized the Court might someday have to square thought-reading technology with the Fourth Amendment.[245] Libertarian pro-gun activists have already devised crude working firearms that a 3D printer can print.[246] Smartphones are beginning to replace lawyers

---

[244] *Id.* at 541 (Breyer, J., concurring in the judgment).

[245] *See* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting). *See also Black Mirror: Crocodile* (Netflix broadcast Dec. 29, 2017) (science-fiction program depicting a device that roughly reads and records a subject's memories for investigative purposes).

[246] *See* Adam Clark Estes, *3D-Printed Guns Are Only Getting Better, and Scarier*, GIZMODO

in simple legal actions, which may someday implicate the Sixth Amendment.[247] Machine-learning software can now convincingly swap faces of subjects in a video;[248] reshape a subject's lip movements to sync with artificially replaced audio;[249] and change the scenes of outdoor photographs to a different season, for example, a summer photo to apparently autumn.[250]

The reality is the Constitution does not exist in a vacuum. "Time works changes, brings into existence new conditions and purposes."[251] New technologies have confounded the existing legal order. In the application of the First Amendment to stolen communications, the "sanctities of . . . home and privacies of life"[252] insist that the law change.

(Jan. 6, 2015), https://gizmodo.com/3d-printed-guns-are-only-getting-better-and-scarier-1677747439 [https://perma.cc/XUZ7-RL6L].

[247] *See* Lily Lou, *This App Helps You Fight Traffic Tickets From Home*, LIFEHACKER (July 7, 2017), https://lifehacker.com/this-app-helps-you-fight-traffic-tickets-from-home-1796682165 [https://perma.cc/SUJ3-FNMU].

[248] *See* Emma Grey Ellis, *People Can Put Your Face on Porn—And the Law Can't Help You*, WIRED (Jan. 26, 2018 7:00 AM), https://www.wired.com/story/face-swap-porn-legal-limbo/ [https://perma.cc/7VBJ-CECJ]; *Face Changer: How to Replace Faces In Video*, WONDERSHARE (Sept. 19, 2017), https://filmora.wondershare.com/video-editing-tips/change-face.html [https://perma.cc/7SQP-LLVJ].

[249] *See* Adam Clark Estes, *Insanely Accurate Lip Synching Tech Could Turn Fake News Videos Into a Real Problem*, GIZMODO (July 12, 2017), https://gizmodo.com/insanely-accurate-lip-synching-tech-could-turn-fake-new-1796843610 [https://perma.cc/34W7-Q6ZR]; *see also* U.S. Pat. Nos. 6,307,576; 6,611,278.

[250] *See* Kevin Stacey, *Photo Editing Algorithm Changes Weather, Seasons Automatically*, NEWS FROM BROWN (Aug. 8, 2014), https://news.brown.edu/articles/2014/08/photo [https://perma.cc/77YP-SBSA].

[251] Olmstead v. United States, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

[252] Boyd v. United States, 116 U.S. 616, 630 (1886).