Privacy, Freedom, and Technology—or "How Did We Get into This Mess?"

*Alex Alben**

I. PRIVACY IS ESSENTIAL FOR INDIVIDUAL FREEDOM

Can we live in a free society without personal privacy? The question is worth pondering, not only in light of the ongoing debate about government surveillance of private communications,[1] but also because new technologies continue to erode the boundaries of our personal space.[2] This Article examines our loss of freedom in a variety of disparate contexts, all connected by the thread of erosion of personal privacy.

In the scenarios explored here, privacy reducing activities vary from government surveillance, personal stalking conducted by individuals, and profiling by data-driven corporations, to political actors manipulating social media platforms. In each case, new technologies and open platforms

* Alex Alben has served as Washington State's Chief Privacy Officer since 2015. As a former technology executive, he focused on legal issues relating to distribution of media over new electronic platforms. He teaches the privacy section of the University of Washington School of Law's tech policy clinic. The author would like to thank Destinee Evers (Seattle University School of Law, Class of 2020) for her research assistance with this Article.

1. *See, e.g.*, Matthew Lynch, *Closing the Orwellian Loophole: The Present Constitutionality of Big Brother and the Potential for a First Amendment Cure*, 5 FIRST AMEND. L. REV. 234 (2007); Christopher Cooke, Note, *Securing Liberty: A Response to Debates on Section 215 of the Patriot Act*, 12 GEO. J.L. & PUB. POL'Y 889 (2014).

2. The erosion of personal space does not appear to completely dissuade consumers. One research firm has estimated that by 2022, twice as many smart devices will be shipped worldwide as were shipped in 2018, for an estimated total of 1.3 billion internet-connected devices. Anick Jesdanun, *Home Items Are Getting Smarter and Creepier, Like It or Not*, AP NEWS (Jan. 7, 2019), https://www.apnews.com/12787de930564f2cbe8fadfdf63e2e7e [https://perma.cc/J5HS-QPAB]. These smart devices include technology that not only monitors the purchasing consumer, but also those who come into contact with them. Google recently introduced a smart doorbell that analyzes the faces of visitors and alerts the homeowner whether or not the visitor is a friend or family member. Samuel Gibbs, *Google Launches Video Doorbell with Facial Recognition in UK*, GUARDIAN (May 30, 2018), https://www.theguardian.com/technology/2018/may/31/nest-hello-google-launches-facial-recognition-data-doorbell-uk-privacy-concerns-amazon-ring [https://perma.cc/7MD9-Y2W5]. Expanding the scope of consumer monitoring, retail chain Walmart recently patented a surveillance technology to record audio of the checkout process. Sam Levin, *Walmart Patents Tech That Would Allow It to Eavesdrop on Cashiers*, GUARDIAN (July 12, 2018), https://www.theguardian.com/business/2018/jul/12/walmart-surveillance-sound-sensors-employees [https://perma.cc/84M6-XDQF].

are used by a bad actor to harm unwitting individuals. Additionally, the affected person has limited legal recourse to avoid the ill effects of intrusion or outright invasion of privacy. Taken together, these examples illustrate the need for new policies and regulation addressing modern threats to privacy and also the requirement to think globally about privacy as a basic right.

II. THE MANIPULATION OF SOCIAL MEDIA PLATFORMS

The vulnerability of data and its potential for political manipulation or misuse was underlined by the well-publicized and well-documented attacks by Russian military and intelligence services on social media platforms, designed to influence American political opinion during the 2016 election and beyond.[3] If "data is the currency" of this century, as Microsoft CEO Satya Nadella has noted,[4] then threats to the integrity of our data go to the core of our ability to function as a society.

In the past year, Facebook has come under increasing pressure to monitor its platform for bad actors who created fake pages and fake advertisements targeting segments of the social network's two billion-person user base.[5] Facebook responded to this criticism by developing enhanced privacy controls,[6] representing a positive step toward giving their users more control over the types of ads they will see and how widely their personal posts are shared. Nevertheless, the underlying platform architecture remains vulnerable to groups that wish to publish false accounts relating to highly charged political issues, such as racism, immigration rights, and even fake news seeking to foment ethnic violence.[7] Facebook has announced that it will hire 10,000 security staff

3. *See* Alicia Parlapiano & Jasmine C. Lee, *The Propaganda Tools Used by Russians to Influence the 2016 Election*, N.Y. TIMES (Feb. 16, 2018), https://www.nytimes.com/interactive/2018/02/16/us/politics/russia-propaganda-election-2016.html [https://perma.cc/MJA4-3X9P]; Kim Zetter, *The Crisis of Election Security*, N.Y. TIMES MAG. (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html [https://perma.cc/T23G-YZ6Y].

4. Satya Nadella, Chief Exec. Officer, Microsoft, Remarks at "Convergence" Conference, New Orleans, La. (Apr. 4, 2016).

5. Taylor Hatmaker, *What We Can Learn from the 3,500 Russian Facebook Ads Meant to Stir up U.S. Politics*, TECHCRUNCH (May 10, 2018), https://techcrunch.com/2018/05/10/russian-facebook-ads-house-intelligence-full-list/ [https://perma.cc/7ST5-X7WV]; *see also* Kathleen Chaykowski, *Facebook Plans to Add 1,000 Moderators Under Pressure to Address Russian Meddling*, FORBES (Oct. 2, 2017), https://www.forbes.com/sites/kathleenchaykowski/2017/10/02/facebook-plans-to-add-1000-moderators-under-pressure-to-address-russian-meddling/#54fca098185a [https://perma.cc/HJ6K-XQDB].

6. Erin Egan, *Giving You More Control of Your Privacy on Facebook*, FACEBOOK NEWSROOM (Jan. 28, 2018), https://newsroom.fb.com/news/2018/01/control-privacy-principles/ [https://perma.cc/2PWU-P2N5].

7. *Frontline: The Facebook Dilemma* (PBS television broadcast Oct. 30, 2018).

and content monitors to address the problem, underlining how large this crisis is for the fourteen-year-old tech company.[8]

These events highlight a structural problem in American law. While a multitude of federal statutes protect individual data sets—such as health care information or student data[9]—the United States lacks a basic privacy right or a privacy law that cuts across wide swaths of personal information.[10]

The right to be secure in our "persons, houses, papers and effects" traces back to the passage of the Fourth Amendment, which became law on March 1, 1792, and was announced by none other than Secretary of State Thomas Jefferson.[11] Because the U.S. Constitution contains no distinct right of privacy, Americans have had to rely on interpretations of the Fourth Amendment to define the extent of privacy rights, creating great uncertainty as to whether government action oversteps the bounds of protected privacy.[12] Not until 2014, for example, did the Supreme Court recognize a distinct privacy right in personal cell phones,[13] and in 2018 a landmark ruling safeguarded cellular data revealing personal locations.[14]

With the evolution of technology, we have mistakenly assumed that we can give up a degree of privacy without a commensurate loss of freedom. Because of our ability to broadcast our "likes" and opinions on Facebook and Twitter, we enjoy a false sense of both agency and autonomy. Yet the manipulation of social media platforms only underscores their vulnerability.[15] In one sense, an open platform such as Facebook is only doing what it was designed to do and fulfill a democratic mission: To allow any person with an Internet connection to create a personal profile and link that profile with others. This process creates a

---

8. Sarah Frier, *Facebook Says It Will Double Safety and Security Staff to 20,000*, BLOOMBERG (Oct. 31, 2017), https://www.bloomberg.com/news/articles/2017-10-31/facebook-says-it-will-double-safety-and-security-staff-to-20-000.

9. *See, e.g.*, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 and 42 U.S.C.); Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2012).

10. For a discussion of the United States' sectoral approach to privacy regulation, see Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 910 (2009); see also Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29 CONN. J. INT'L L. 257, 289–90 (2014).

11. RICHARD LABUNSKI, JAMES MADISON AND THE STRUGGLE FOR THE BILL OF RIGHTS 222–23 (2006).

12. Schwartz, *supra* note 10.

13. *See* Riley v. California, 573 U.S. 373 (2014).

14. *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

15. For example, Facebook shared the personal data of its users to commercial "partners" without user consent in order to provide targeted advertising. Gabriel J.X. Dance, Michael LaForgia & Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html.

"virtuous circle network effect" when the platform reaches a critical mass of users, encouraging more people to join and discouraging entry of competitors into the market to challenge the leader's supremacy. Even under attack, Facebook has continued to gain users on a global basis.[16]

There is an odd note to the criticism that Facebook must do a better job regulating speech and controlling what can and cannot be said by its users. Facebook, after all, is not a media company. It was founded by tech geeks in a college dorm, eager to create a tool to allow college students—initially in the Ivy League and Stanford—to see each other's photos. Facebook's first thousand employees had skill sets undoubtedly centered on web architecture and distribution of media in a networked environment. When founded in 2004, Mark Zuckerberg probably never dreamed that Facebook would become a major source of news for billions of users or that he would be called upon to adjudicate issues such as what constitutes unacceptable "hate speech."[17]

Facebook in many ways is a victim of its own success. A platform of two billion connected users might seem to resemble a "utility" or an essential communications technology, such as electricity or a phone system.[18] A company that knows tens of thousands of things about each of its users might appear to pose a general threat to individual privacy, even if its core economic interest is simply to market goods and services to individuals based on their personal habits. Yet, as Facebook's business model evolved, it became increasingly data-driven in order to serve third party advertisers—placing a premium on collecting and keeping as much information as it could about its users in order to gain a competitive edge against competitors such as Google and Twitter.[19]

Mr. Zuckerberg infused Facebook with a mission to "make the world more open and connected," when his founding team turned on the lights.[20] This ethos allowed both legitimate and illegitimate actors to populate the Facebook neighborhood. It appealed to a libertarian sensibility that people

---

16. Josh Constine, *Facebook Shares Climb Despite Q3 User Growth and Revenue*, TECHCRUNCH (Oct. 30, 2018), https://techcrunch.com/2018/10/30/facebook-earnings-q3-2018/ [https://perma.cc/SEG3-VWGE].

17. *Sasse to Zuckerberg: Define Hate Speech*, WASH. POST (Apr. 10, 2018), https://www.washingtonpost.com/video/politics/sasse-to-zuckerberg-define-hate-speech/2018/04/10/857cc8d2-3d04-11e8-955b-7d2e19b79966_video.html?utm_term=.afc7e26883ec.

18. K. Sabeel Rahman, *Regulating Informational Infrastructure: Internet Platforms as the New Public Utilities*, 2 GEO. L. TECH. REV. 234 (2018).

19. Dance, LaForgia & Confessore, *supra* note 15.

20. Mark Zuckerberg, *Bringing the World Closer Together*, FACEBOOK (June 22, 2017), https://www.facebook.com/notes/mark-zuckerberg/bringing-the-world-closer-together/10154944663901634/ [https://perma.cc/6WZS-S3RQ]; *see also* Kathleen Chaykowski, *Mark Zuckerberg Gives Facebook a New Mission*, FORBES (June 22, 2017), https://www.forbes.com/sites/kathleenchaykowski/2017/06/22/mark-zuckerberg-gives-facebook-a-new-mission/#5d5419001343 [https://perma.cc/H6HV-Y7F3].

should be able to do and say what they want in their personal lives and to express themselves on their chosen platform. Yet, as Facebook's platform grew and emerged as a dominant source of news and information for its users, it developed the need for codes of conduct for acceptable behavior and ultimately some sort of internal governing mechanism to enforce those codes of conduct. The company developed software filters to combat the publication of pornography and other socially unacceptable content and, in that process, came to resemble more of a public forum and less of a private communications network.[21] At a fundamental level, how was Facebook supposed to answer the question of "Whose social norms should a global company seek to enforce?" With diverse users living in Saudi Arabia, China, and Canada, it is not easy to see how Facebook or any social media company could ever satisfy all of its disparate and divergent constituencies.

Nevertheless, with the well-documented revelations of manipulation by Russians and political groups fomenting violence in Pakistan and Myanmar, Facebook can no longer maintain the pose that any member could determine social norms and acceptable behavior. It is no longer just a tech company. It is now a media company and news organization, whether or not it ever wished to become one. As such, Facebook has to continuously and rapidly monitor and control user behavior on its sites in order to promote political neutrality and to filter out those who wish to abuse its founding notions of openness and transparency.

Protection of privacy constitutes the soft underbelly of Facebook's value. The platform attracts users and advertisers because of its ability to connect individuals based on their profiles. On an atomistic level, each user might feel "safe" to navigate his or her own connections across the platform. Yet, when everyone's profiles become aggregated and then dissected by Artificial Intelligence and other analytic tools, the platform becomes vulnerable to manipulation because it represents such a large and open target. This paradox will persist. If Facebook's management pushes too hard against the open side of its equation, then it will limit revenue and future growth. If it continues to allow unchecked growth, then the credibility of content on the site will come under attack and users will turn off or tune out. External regulation of its privacy practices may actually help the company strike this difficult balance by fostering rules that allow for more user control and ultimately less platform manipulation.

21. *Community Standards Enforcement Report*, FACEBOOK (Nov. 2018), https://transparency.facebook.com/community-standards-enforcement [https://perma.cc/7GFN-27NF].

III. TECH COMPANIES PUSH BACK AGAINST BIG BROTHER

The other side of the privacy and freedom coin features a traditional enemy of privacy—big government. As if it were not enough that tech companies have grappled with the new set of challenges posed by the success of their platforms and software applications, they also have emerged as important actors in the long-standing debate over the privacy of personal communications.

Only in the past few years have American tech companies such as Apple and Microsoft publicly and prominently pushed back against the federal government's attempts to access personal conversations via electronic communications.[22] What accounts for this contradiction?

At the most abstract level, experts tend to frame the debate in terms of *privacy vs. security*, focusing on the relatively rare cases where the government is seeking to intercept or open an individual's emails, texts, or personal records. The government makes its case, arguing that it must vigorously pursue its duty to solve crimes and keep us safe from terrorist attacks and other threats to public safety. During the era when the Patriot Act reigned with wide latitude—roughly from 2001 through most of 2015—the federal government enjoyed extraordinary powers to collect the bulk data labels that encapsulate phone calls and emails.[23] Subjecting such data to mathematical analysis, our security agencies then determined whether they needed to request a special warrant to read the content of the communications.

This controversy came to a head in several cases that pitted the Department of Justice, acting on behalf of the FBI, against Apple Computer, with Apple maintaining that it needs to protect the privacy rights of its customers and therefore will not go to extraordinary lengths to open encrypted phones. One New York magistrate ruled that the FBI had no right to ask an American company to break into its own phones and violate the private communications of its customers.[24] The judge vociferously stated that it was absurd for the FBI to try to apply the All Writs Act, passed in 1789, to ask a modern technology company to write computer code to further the execution of a law enforcement action.[25]

In the better known California case, Apple lost the early rounds of the proceedings, with the federal court holding that it should be compelled

---

22. For recent litigation, see United States v. Microsoft Corp., 138 S. Ct. 1186 (2018); *In re* Search of an Apple iPhone, No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016) (order compelling Apple, Inc. to assist agents in search).

23. *See* Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1, 12–14 (2014).

24. *In re* Apple, Inc., 149 F. Supp. 3d 341, 376 (E.D.N.Y. 2016).

25. *Id.*

to open the iPhone of terrorist suspect Syed Rizwan Farook, who, along with his wife, perpetrated the San Bernardino rampage that killed fourteen people and wounded twenty-two in December of 2015.[26] The FBI seized three iPhones from Farook, one of which was an iPhone issued by his employer, which he apparently used for communication related to his job at the County Department of Health.[27] This iPhone 5c had security measures that prevented multiple attempts to "brute force" a guess of the phone's four-digit passcode.[28] While the legal case was pending, the FBI found a hacker who was able to circumvent the software that limited the phone's passcode entry function, enabling the FBI to randomly generate the correct code.[29] Not surprisingly, Farook's work phone did not contain the type of valuable information the FBI had hoped would lead them to advance their investigation into the motives and network of Farook and his spouse, who both died in a shootout after the attack.

In the case of *United States v. Microsoft Corp.*,[30] Microsoft staunchly resisted a DOJ subpoena for emails stored by Microsoft's Hotmail email service on a computer server in Ireland.[31] Microsoft maintained that our domestic DOJ subpoenas should not have extraterritorial effect.[32] The Justice Department countered that, in an age of cloud computing, such data was only a few computer clicks away from Microsoft's platform controllers and could rapidly be retrieved.[33] Physical location, in this sense, no longer matters in an era of universal bit storage in virtual environments.[34] While the Microsoft case was pending after a hearing in the Supreme Court in February of 2018, Congress passed the CLOUD Act, resolving the matter in a way that allows the DOJ to access some data stored overseas, but with privacy protections largely determined by the local law of the foreign country.[35]

In these dramatic cases it is tempting to conclude that the key issue is a balance between privacy interests and national-security interests, but this might not be the most useful way to frame the problem. The FBI seeks to decrypt the communication devices of terrorists in extraordinary cases.

---

26. *See In re Apple iPhone*, 2016 WL 618401.

27. *See generally* Danny Yadron, *San Bernardino iPhone: U.S. Ends Apple Case After Accessing Data Without Assistance*, GUARDIAN (Mar. 29, 2016), https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone [https://perma.cc/N42P-DN7L].

28. *See generally id.*

29. *See generally id.*

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

31. *Id.*

32. *Id.* at 1187.

33. *Id.*

34. *Id.*

35. *See* Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub. L. No. 115-141, div. V, 132 Stat. 348, 1213–25 (2018) (codified in scattered sections of 18 U.S.C.).

In the normal course, Apple users text and phone their friends, families, and business contacts tens of millions of times a day.[36] Our judicial system has proven methods to resolve the edge cases where the FBI asks a company to do something extraordinary, such as write a new program to defeat its own software. Whether or not a technology company or the DOJ wins or loses a particular case of this nature does not detract from the principle that private communications of American citizens should remain private.

Citizens of other countries would consider it a luxury to live in a society where technology companies have redress to the courts to try to prevent the government from snooping on private communications. In modern day Iran or China, for example, citizens cannot freely assemble or vocally protest government actions without becoming targets for surveillance or imprisonment.[37] When a citizen is shadowed by secret police and beaten when seeking to make court appearances to defend dissidents, the notion of privacy ceases to exist. In today's Russia, hundreds of courageous investigative journalists and vocal political opponents have been jailed or murdered.[38] In China, the state arrests human rights lawyers on the courtroom steps. Additionally, it has initiated a program of mass incarceration of the Uyghur ethnic group in Western China without any recourse to the courts.[39]

There is very little latitude to protest policy in such societies, where the government determines the extent of personal freedom to conduct such protests. Privacy is often the first casualty in the persecution of ordinary people who dare to stray from the official party line.

---

36. Kif Leswing, *Apple Says People Send as Many as 200,000 iMessages per Second*, BUS. INSIDER (Feb. 12, 2016, 2:08 PM), https://www.businessinsider.com/eddy-cue-200k-imessages-per-second-2016-2 [https://perma.cc/FL5N-AQMY].

37. *See generally* IAN VÁSQUEZ & TANJA PORČNIK, THE HUMAN FREEDOM INDEX 2018: A GLOBAL MEASUREMENT OF PERSONAL, CIVIL, AND ECONOMIC FREEDOM (2018), https://object.cato.org/sites/cato.org/files/human-freedom-index-files/human-freedom-index-2018-revised.pdf [https://perma.cc/Y9G9-36P8].

38. *See generally 58 Journalists Killed in Russia*, COMM. TO PROTECT JOURNALISTS, https://cpj.org/data/killed/europe/russia/?status=Killed&motiveConfirmed%5B%5D=Confirmed&type%5B%5D=Journalist&cc_fips%5B%5D=RS&start_year=1992&end_year=2019&group_by=location [https://perma.cc/93HX-F5S5]; *A List of Murdered Russian Journalists That Moscow Says It Didn't Kill*, HAARETZ (May 30, 2018, 3:55 PM), https://www.haaretz.com/world-news/europe/a-list-of-murdered-russian-journalists-that-moscow-says-it-didn-t-kill-1.6133887 [https://perma.cc/T98J-MUSX].

39. *See generally* Eva Dou, Jeremy Page & Josh Chin, *China's Uighur Camps Swell as Beijing Widens the Dragnet*, WALL ST. J. (Aug. 17, 2018, 3:41 PM), https://www.wsj.com/articles/chinas-uighur-camps-swell-as-beijing-widens-the-dragnet-1534534894.

IV. FAKE NEWS AS AN INVASION OF PRIVACY

Even in our terribly warped media environment, a conspiracy theory holding that the Sandy Hook parents faked the deaths of their children stands out as ugly and offensive. Promulgated by right-wing media outlets, such as radio personality Alex Jones, the theory alleged that rather than reacting to the tragic school shooting that took twenty-six lives in 2012, the Sandy Hook parents were actually actors and that the event had been staged.[40] In early 2018, several parents filed three defamation lawsuits against Alex Jones, host of *Infowars*, to combat this venomous perversion of the deaths of twenty schoolchildren and six teachers at the hands of a mentally ill young man in Newtown, Connecticut.[41]

Unfortunately, current state privacy and defamation laws make it very difficult for plaintiffs to prevail in cases where the stated facts are wrong but the subjects of the controversy have become public figures. This dates back to the famous case of *Time, Inc. v. Hill*, where a family was thrust into the public eye in 1952 after being taken hostage in a Philadelphia suburb for nineteen hours.[42] To publicize a new Broadway play about the incident, *Life Magazine* published an account of the hostage taking that distorted certain facts about the actual events.[43] To get out of the public eye, the Hills moved their family out of state and sought to protect their privacy to allow their children to grow up in peace.[44] Yet, their story became the subject of a novel, *The Desperate Hours*; a popular film starring Humphrey Bogart; and a Broadway play.[45] Then *Life Magazine* took up the case three years later and thrust the Hills back into the public eye.[46] The Hills had not claimed defamation by *Life Magazine*, but simply that the iconic American magazine had not done the fact checking to accurately report their story.[47]

In one of the most important cases in over two hundred years of American jurisprudence involving the privacy rights of private individuals appearing in news stories, the U.S. Supreme Court decided in January of 1967 that the Hills could not prevail on a "false light" privacy claim.[48] Future President Richard Nixon argued the case on behalf of the Hill

40. Elizabeth Williamson, *Judge Rules Against Alex Jones and Infowars in Sandy Hook Lawsuit*, N.Y. TIMES (Aug. 30, 2018), https://www.nytimes.com/2018/08/30/us/politics/alex-jones-infowars-sandy-hook-lawsuit.html.

41. *Id.*

42. Time, Inc. v. Hill, 385 U.S. 374 (1967).

43. *Id.* at 377–78.

44. *Id.* at 378.

45. *Id.* at 377–78.

46. *Id.*

47. *Id.* at 378.

48. *Id.* at 396.

family, doing a masterful job of distinguishing why the family deserved the right to sue for damages. In a famous exchange, Nixon plaintively asked Justice Hugo Black, "[a]re private persons, involuntarily drawn into the vortex of a public issue . . . allowed, in effect, to be used as gimmicks for commercial purposes in a falsified situation . . . ?"[49] Justice Black and his fellow jurists disagreed with Nixon and his clients.[50] By a 5–4 vote, the Court missed the boat, putting an absolute premium on the magazine's First Amendment rights.

Had the Court recognized the violation of privacy presented before it, our privacy laws would have been strengthened immeasurably for the following generations, serving as a guiding light for the era of digital technology and the host of devices and apps that threaten personal privacy. Having to guard against meritorious suits brought by individuals, protection of privacy rights might have limited the evolution of our current age of "fake news."

I have opined that *Time, Inc. v. Hill* was wrongly decided and that our courts should give victims redress from false stories, even when the individuals have been thrust into the public eye against their will.[51] The Sandy Hook case is a prime example of the hole in our law that allows media outlets to spew false narratives about private individuals. Referring to the Second Amendment, radio host Alex Jones said, "It is every American's right to question any big event, especially when it's seized on to take the basic liberties of Americans . . . ."[52] Yet, no one is questioning the right of journalists to ask questions about important stories. At stake here is the ability of ideologues to promote false facts and then hide behind the First Amendment when they harm private individuals. Let's hope that our courts vindicate the Sandy Hook families, who never should have been forced to experience this second nightmare.

In the meantime, we need to think more deeply about correcting the basic flaw in American law relating to privacy and develop a theory of privacy as a "human right" akin to the European and other models.

---

49. SAMANTHA BARBAS, NEWSWORTHY: THE SUPREME COURT BATTLE OVER PRIVACY AND PRESS FREEDOM 222 (2017).

50. *Time, Inc.*, 385 U.S. at 398.

51. *See generally* Alex Alben, *Privacy and the Press—An Examination of how the Supreme Court Confused Press Freedom and False Light Privacy in Critical Cases*, 26 STAN. L. & POL'Y REV. 13 (2017).

52. Leslie Brody, *Sandy Hook Parents Sue Radio Host Alex Jones for Calling Shooting a Hoax*, WALL ST. J. (Apr. 17, 2018), https://www.wsj.com/articles/sandy-hook-parents-sue-radio-host-alex-jones-for-calling-shooting-a-hoax-1524000776.

V. MODERN TECHNOLOGY ENABLES HARASSMENT AND STALKING, WITH VERY LITTLE RECOURSE FOR VICTIMS

Stalking represents a real and present danger in the physical world and in online settings. In 2014, *Atlantic Magazine* reported that one-third of women reported being threatened or stalked on the web.[53] After an individual—a woman in the vast majority of cases—seeks to terminate an acquaintance or relationship, her privacy is in jeopardy. Stalkers can use public records requests to find the physical and work addresses of their targets.[54] Hackers can trace online photographs and postings like many digital footprints. Victims of stalking often have to erase personal histories, get new phone numbers and, in dramatic cases, physically move to shield themselves and their loved ones from a stalker's pursuit.[55] While some states have passed so-called "revenge porn" statutes, the general vulnerability of women to online harassment has not been adequately addressed, either in law or public policy.[56]

In cases of stalking and harassment, privacy becomes essential for a person to live her life with a degree of autonomy, even if that is simply the freedom not to worry that a creepy guy is intruding on her online profile. In too many cases, the stalker succeeds in violating a target's physical space, leading to physical crimes. Cyberstalking, like political persecution, underlines the importance of safeguarding a zone of personal privacy in the conduct of our daily lives.

But what about less dramatic cases? The zone of privacy surely is not delimited by political causes or concerns for personal safety.[57] The ubiquitous spread of municipal surveillance cameras and police body cameras makes it likely that the movements of average citizens in public spaces will be recorded, tracked, and retained for future analysis for years.

These technologies highlight the point that Emily Dickinson tried to make 140 years ago: Privacy is our natural state; public exposure is

---

53. Marlisse Silver Sweeney, *What the Law Can (and Can't) Do About Online Harassment*, ATLANTIC (Nov. 12, 2014), https://www.theatlantic.com/technology/archive/2014/11/what-the-law-can-and-cant-do-about-online-harassment/382638/ [https://perma.cc/JS7S-ZL6D].

54. *Stalking Information*, STALKING RESOURCE CENTER, http://victimsofcrime.org/our-programs/stalking-resource-center/stalking-information [https://perma.cc/WF4C-DRBJ].

55. *See generally* Sweeney, *supra* note 53.

56. *See, e.g.*, WASH. REV. CODE § 9A.86.010 (2018). *See generally* Sweeney, *supra* note 53.

57. Technology can also lead to privacy risks for dating apps. In early 2018, it was discovered that a popular dating app for gay men was sharing its users' HIV status data with third-party vendors. *Grindr Shared Information About Users' HIV Status with Third Parties*, GUARDIAN (Apr. 3, 2018), https://www.theguardian.com/technology/2018/apr/03/grindr-shared-information-about-users-hiv-status-with-third-parties [https://perma.cc/MUP9-EPVB]. After public pressure, the company modified its information-sharing practices.

artificial.[58] Giving up privacy should be a conscious choice, not a special exemption from the norm.

VI. DIGITAL DEVICES, THE INTERNET OF THINGS, AND TECH PLATFORMS

Most of us using digital devices connected to networks regularly share large swaths of data about our personal habits, entertainment choices, and geolocation with unseen marketers, to be used in ways we have not authorized and may not even understand.[59] Our behavior as consumers suggests that we will continue to allow for the widespread dissemination of our personal information on a broad new range of platforms, including Internet-connected devices. Email—both personal and corporate—is increasingly vulnerable to attack;[60] yet, we treat it quite casually and do not contemplate the scenarios where it can be used against us, our employers, or our country.

The same platforms that allow us to organize for a candidate or "meet up" to do volunteer service can be used by governments or interlopers to monitor our movements and limit the exercise of our rights.

In sum, we have failed to connect the dots between this loss of privacy—some of it voluntary—and constraints on our personal freedom. Privacy means much more than the right not to be preyed upon or secretly watched. Our privacy not only erodes when the law enforcement exceeds its authority or a stalker targets us but also when we allow our personal zones of privacy to shrink in favor of commerce and convenience.

VII. SOLUTIONS

In order to create a defensible zone of privacy, we will need to define it more clearly for the new technologies that continue to shape our digital environments. This will include geolocation data for both cell phones and automobiles, biometric identifiers, and vast video archives of our movements around our neighborhoods and highways. We will need to establish much more overt forms of personal consent to such practices, whether on the part of government, corporations, or social media. We may even need to move toward a more European model, which recognizes the importance of data protection as a core human right.[61]

---

58. *See generally* EMILY DICKINSON, *I'm Nobody, Who Are You*?, *in* THE POEMS OF EMILY DICKINSON (Ralph W. Franklin ed., Harvard University Press 1998) (1891).

59. *See generally* Jamie Lee Williams, *Privacy in the Age of the Internet of Things*, 41 HUM. RTS., no. 3, 2016, at 14.

60. Josephine Wolff, *The Most Shocking Thing About Encrypted Email Being Vulnerable Is That Anyone Still Uses Encrypted Email*, SLATE (May 15, 2018), https://slate.com/technology/2018/05/pgp-and-s-mime-are-vulnerable-but-also-no-one-used-them-anyway.html [https://perma.cc/NZL4-WKNZ].

61. Schwartz, *supra* note 10, at 274.

If we fail to get ahead of the technology curve, we will find ourselves with shrinking zones of privacy in all aspects of our lives and become more vulnerable to our own data being used against us, risking our personal freedom. And by the time we recognize this loss it will be too late to recover this essential aspect of our humanity. In sum, this Article has attempted to outline the following trends facing our social media and traditional media environments:

*Privacy is not only under pressure from government surveillance but also corporate profiling and unintended uses.

*When big corporate platforms—such as Facebook or Twitter—come under attack, privacy suffers when identity is compromised, and speech rights suffer when identity becomes distorted. The experience of the 2016 election established this.

*Lack of clear privacy law enables attacks against individuals who cannot control the media messages propagated against them.

*Victims of harassment and stalking need more overt policy and protection to prevent abuse of technologies that enable such behaviors.

In each of these cases, the solutions will encompass a better governance model for corporate technology platforms that serve as speech forums and information delivery channels. Broad regulatory regimes—such as the European Union's General Data Protection Regulation (GDPR)—will probably have a net positive effect for both freedom and democracy, to the extent that individuals regain control over their personal information and such information becomes less vulnerable to manipulation. Yet the threat will be with us for many years to come; advocates of privacy and democracy must remain vigilant.