INTRODUCTION

Lore has it that the internet was born on an autumn night in 1969.[1] Sitting in front of a computer at the University of California in Los Angeles, Professor Leonard Kleinrock sent a message to another computer housed at the Stanford Research Institute in Palo Alto: "LO."[2] Kleinrock had intended to write "LOGIN," but the system crashed after the first two letters were transmitted.[3] Nonetheless, sending "LO" was an incredible success and marked the beginning of a monumental — and unbelievably swift — societal shift.

Although the exponential growth of internet and computer use was not a surprise to many technologists,[4] the statistics are striking: As of 2016, about 81% of adults in the United States have a smartphone,[5] and 87% of U.S. adults use the internet.[6] In 2017, the average U.S. adult spent over four hours per day on her phone.[7] Seventy-nine percent of U.S. adults shop online as of 2016, up from only 22% in 2000.[8] By 2015, 65% of U.S. adults used social media, up from 7% in 2005, including 90% of young adults aged eighteen to twenty-nine.[9] And by 2012, 71% of smartphone users said that they could not go a day without their phones.[10] Nearly one-third said that their phone was the first thing they looked at in the morning, and the last thing they looked at in the evening.[11]

---

[1] Oliver Burkeman, *Forty Years of the Internet: How the World Changed for Ever*, THE GUARDIAN (Oct. 23, 2009, 3:00 PM), https://www.theguardian.com/technology/2009/oct/23/internet-40-history-arpanet [https://perma.cc/UA83-N7M5].

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] Jacqueline Howard, *Americans Devote More than 10 Hours a Day to Screen Time, and Growing*, CNN (July 29, 2016, 4:22 PM), http://www.cnn.com/2016/06/30/health/americans-screen-time-nielsen/index.html [https://perma.cc/3KHE-KTH6].

[6] Monica Anderson & Andrew Perrin, *13% of Americans Don't Use the Internet. Who Are They?*, PEW RES. CTR. (Sept. 7, 2016), http://www.pewresearch.org/fact-tank/2016/09/07/some-americans-dont-use-the-internet-who-are-they [https://perma.cc/5PJK-YA5C].

[7] *How Much Time Do People Spend on Their Mobile Phones in 2017?*, HACKER NOON (May 9, 2017), https://hackernoon.com/how-much-time-do-people-spend-on-their-mobile-phones-in-2017-e5f90a0b10a6 [https://perma.cc/N36M-HV42].

[8] Aaron Smith & Monica Anderson, *Online Shopping and E-Commerce*, PEW RES. CTR.: INTERNET & TECH. (Dec. 19, 2016), http://www.pewinternet.org/2016/12/19/online-shopping-and-e-commerce/ [https://perma.cc/64YS-774G].

[9] Andrew Perrin, *Social Media Usage: 2005–2015*, PEW RES. CTR.: INTERNET & TECH. (Oct. 8, 2015), http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015 [https://perma.cc/2W5F-VHTT].

[10] *See Your Wireless Life: Results of TIME's Mobility Poll*, TIME, http://content.time.com/time/interactive/0,31813,2122187,00.html [https://perma.cc/FQ9C-5WP4].

[11] *Id.*

It is clear that in the fifty years since "LO," and the roughly twenty-five years since the first usable internet browser was launched,[12] internet-connected computers have become a critical part of everyday life. In the words of Steve Crocker, a computer scientist who was present for that first internet communication in 1969, "there has not been, in the entire history of mankind, anything that has changed so dramatically as computer communications, in terms of the rate of change."[13]

In our growing reliance on modern technology, smartphone and computer users are placing more and more of their personal data on devices and online — both purposefully, by storing photos and documents, for example, and unwittingly, by communicating personal preferences to advertisers, for example. And yet most users do not completely understand what they have gotten themselves into. Take, for example, a 2012 survey gauging how much the average U.S. adult understands about cloud storage and computing.[14] A majority of respondents, 54%, asserted that they had never used the cloud.[15] However, researchers found that 95% of this group actually *did* use the cloud — when shopping, banking, using social media, playing games, storing photos, and engaging in other activities.[16] Further, the survey found that 22% of U.S. adults pretend to know what the cloud is and how it works even though they do not, and 56% suspect that others are doing the same.[17] (For the record, "the cloud" refers to a network of servers located around the world, which are used to "store and manage data, run applications, or deliver content" to internet-connected devices.[18] It bears no relation to actual clouds.)

Unsurprisingly, the law is struggling to catch up with these developments as well. This edition of *Developments in the Law* considers issues that arise when our personal information is stored on computers and online. Chapters I and II address the rise of surveillance intermediaries[19]: tech companies that store an enormous amount of their users' personal data. In storing this data, these companies have become critical

---

[12] Matthew Lasar, *Before Netscape: The Forgotten Web Browsers of the Early 1990s*, ARS TECHNICA (Oct. 11, 2011, 10:15 AM), https://arstechnica.com/information-technology/2011/10/before-netscape-forgotten-web-browsers-of-the-early-1990s [https://perma.cc/GVE9-HWVT].

[13] Burkeman, *supra* note 1.

[14] Jay Yarow, *51% of People Think Stormy Weather Affects "Cloud Computing,"* BUS. INSIDER (Aug. 30, 2012, 12:14 PM), http://www.businessinsider.com/people-think-stormy-weather-affects-cloud-computing-2012-8 [https://perma.cc/9PZN-GYW6].

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *What Is the Cloud?*, MICROSOFT: AZURE, https://azure.microsoft.com/en-us/overview/what-is-the-cloud [https://perma.cc/HE43-EG38].

[19] The term "surveillance intermediaries" was coined in a recent article by Professor Alan Rozenshtein. *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 104–05 (2018).

to our law enforcement and national security apparatus on the one hand, and to our privacy on the other. Chapter III turns its attention to reader privacy, advocating for the creation of federal reader privacy legislation in our age of e-readers and ever-available search histories. Finally, Chapter IV asks how the legal requirements of wills — which were developed prior to the rise of the internet — can be adapted to "electronic wills." Together, these Chapters address a wide range of novel legal issues and needs that have arisen in the wake of "LO."

Chapter I begins by noting that surveillance intermediaries hold an extraordinary amount of power in our law enforcement and national security apparatus.[20] These companies have significant discretion in deciding when to cooperate with government requests for their users' personal data, and when to resist such requests.[21] The Chapter suggests that leaving such discretion to private, profit-motivated companies may be problematic and that this might be an area for future regulation.[22] Before Congress can regulate intermediary behavior, it must understand the incentive structure motivating that behavior: "How do surveillance intermediaries decide when to cooperate and when to resist? And how do these decisions vary between companies and over time?"[23]

The rest of the Chapter sets out to answer these questions. It observes that existing scholarship seeks to generalize the behavior of surveillance intermediaries, arguing either that intermediaries tend to *assist* the government, largely cooperating with government investigations (whether or not they are legitimate), or that intermediaries tend to *resist* the government, obstructing government investigations (whether or not they are legitimate).[24] But this is a false dichotomy — the Chapter shows that intermediaries do both, and that the decision of whether to assist or resist the government varies between companies and over time.[25] Next, the Chapter explores several incentives that might cause a surveillance intermediary to assist or resist a government investigation.[26] These incentives include a company's reactions to current events,[27] technical structure,[28] and business model,[29] as well as the interests of corporate and individual users.[30]

---

[20] *See infra* ch. I, pp. 1722–23.
[21] *Id.*
[22] *Id.* at 1723–24.
[23] *Id.*
[24] *Id.* at 1724–27.
[25] *Id.* at 1727–29.
[26] *Id.* at 1729–36.
[27] *Id.* at 1730–32.
[28] *Id.* at 1732–34.
[29] *Id.* at 1734–35.
[30] *Id.* at 1735–36.

Finally, the Chapter ends on a hopeful note: Although the surveillance intermediary model is not ideal, it is not without its advantages.[31] When large companies act as surveillance intermediaries, they can generate public information about surveillance practices,[32] leverage their bird's-eye view into federal, state, and local surveillance regimes,[33] pursue surveillance-related litigation unavailable to individuals,[34] invest resources in policy teams that handle government requests for data,[35] and serve as valuable resources to the government, particularly in the face of emergencies.[36]

Chapter II also discusses the role of surveillance intermediaries, this time in the context of challenging national security–related surveillance in court. It begins by considering the following scenario: Under § 702 of the Foreign Intelligence Surveillance Act[37] (FISA), the U.S. government can conduct surveillance on any non-U.S. person.[38] Under the Fourth Amendment, the U.S. government cannot conduct surveillance on any U.S. person, unless that surveillance is pursuant to a search warrant.[39] However, when a U.S. person exchanges emails with a non-U.S. person, and that non-U.S. person is subject to surveillance under § 702, the U.S. person's emails will be "incidental[ly] collect[ed]" as part of that surveillance.[40] So when the U.S. government requests that Google produce records related to the non-U.S. person's email account, Google's compliance will include emails sent to that account by a U.S. person. The central question of this Chapter is: how can that U.S. person challenge the incidental collection of her data?[41]

The answer is that she likely would not have standing to pursue such a challenge — but the surveillance intermediary, Google, would. In *In re Directives*,[42] the Foreign Intelligence Surveillance Court of Review concluded that surveillance intermediaries have standing to challenge

---

31 *Id.* at 1737–41.

32 *Id.* at 1738.

33 *Id.* at 1738–39.

34 *Id.* at 1739.

35 *Id.*

36 *Id.* at 1740.

37 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 18 and 50 U.S.C.).

38 *See* 50 U.S.C. § 1881a (2012 & Supp. III 2016); *see also infra* ch. II, p. 1742 (defining U.S. persons as "American citizens located within U.S. borders, American citizens located abroad, and foreign nationals who are either on U.S. soil, and/or who have developed 'substantial ties' to the United States").

39 *Infra* ch. II, p. 1742.

40 *Id.* at 1743.

41 *Id.*

42 *In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).

§ 702 surveillance: intermediaries must devote resources toward complying with surveillance requests and therefore can show an injury in fact.[43] In contrast, the Supreme Court concluded that individuals do *not* have standing in these cases. In *Clapper v. Amnesty International USA*,[44] the Court held that individuals who suspect that they are subject to incidental collection cannot show an adequate concrete injury under the standing doctrine.[45]

The Chapter goes on to argue that individuals must be permitted to pursue surveillance challenges themselves. It first explains why surveillance intermediaries cannot be relied upon to vindicate the privacy rights of their users — intermediaries' incentives will not always align with those of their customers subject to incidental collection, and being a privacy advocate is simply not the job of a profit-motivated company.[46] Second, it explains the benefits of allowing an individual to be her own advocate[47] and concludes with some suggestions for how standing doctrine might be able to accommodate such suits.[48]

Chapter III considers another privacy issue related to personal data: the need for federal reader privacy legislation. It begins by noting that our video-consumption habits — both off- and online — are protected by the Video Privacy Protection Act[49] (VPPA).[50] Passed in 1988, the VPPA was created as "a unique gap-filler, extending protection . . . to the expressive activities recognized as vital to the First Amendment but left underprotected by the Fourth."[51] However, our book- and eBook-consumption habits are offered no such statutory protection.[52] This Chapter argues that the VPPA, though not perfect, is a good model for badly needed federal reader privacy legislation.[53]

First, the Chapter argues that the VPPA has aged surprisingly well.[54] The VPPA's flexible language has allowed the statute to be applied to both VHS tapes and online streaming services, surviving significant technological changes.[55] In addition, the VPPA's close relationship with the First Amendment has allowed it to remain a powerful statute despite changes to standing doctrine.[56] Next, the Chapter addresses the real

---

[43] *Infra* ch. II, pp. 1748–50.
[44] 568 U.S. 398 (2013).
[45] *Infra* ch. II, pp. 1750–52.
[46] *Id.* at 1752–60.
[47] *Id.* at 1760–63.
[48] *Id.* at 1763–65.
[49] 18 U.S.C. § 2710 (2012).
[50] *Infra* ch. III, p. 1767.
[51] *Id.* at 1768.
[52] *Id.* at 1783.
[53] *Id.* at 1783–89.
[54] *Id.* at 1769.
[55] *Id.* at 1769–70.
[56] *Id.* at 1770–77.

weakness of the VPPA: poor drafting, which has led to numerous issues of statutory interpretation.[57] While these are real problems, they are not inherent to the structure of the VPPA; they could easily be fixed with more accommodating statutory interpretation.[58]

Finally, the Chapter returns to its call for federal reader privacy legislation modeled off of the VPPA and its First Amendment bent.[59] It argues that such legislation is needed, among other reasons, because reader privacy legislation would "implicate[] First Amendment values that the First Amendment cannot protect."[60] Problems arise because "[t]he First Amendment governs state action, but citizens are increasingly surveilled not by state actors, but by private corporations who render the need for direct government surveillance of such activity redundant."[61] In other words, the First Amendment on its own cannot extend its protections in order to combat the chilling effect of surveillance by private companies — which is precisely why federal reader privacy legislation is so badly needed. The Chapter concludes that the VPPA's flexibility in the face of technological and doctrinal changes, and the ease with which its flaws could be addressed, make the VPPA the ideal candidate for a model for federal reader privacy legislation.[62]

Finally, Chapter IV considers how the process of creating a will can be modernized to reflect the reality that most people are now accustomed to storing their data on computers and the internet. In order to create and execute a valid will, a testator must follow three "formalities": the will must be in writing, signed, and attested to.[63] Due to the rise of computer and internet use, probate courts increasingly must evaluate the validity of "electronic wills" — "wills that have been written, signed, and/or attested using an electronic medium."[64] However, it is thus far unclear how the traditional formalities of a will can be translated to an electronic medium, and scholars cannot seem to agree on a path forward.[65]

This Chapter seeks to illuminate such a path by providing an analytic framework with which to evaluate the validity of an electronic will. First, the Chapter considers the current requirements for valid wills.[66]

---

[57] *Id.* at 1777–83.
[58] *Id.* at 1782–83.
[59] *Id.* at 1783–87.
[60] *Id.* at 1784.
[61] *Id.*
[62] *Id.* at 1786–87.
[63] *Infra* ch. IV, p. 1790.
[64] *Id.*
[65] *Id.* at 1790–91.
[66] *Id.* at 1792–95.

It describes the functions that will formalities serve[67] and current compliance standards that wills must meet in order to satisfy those formalities.[68]

Second, the Chapter considers how these formalities might be applied to electronic wills.[69] It observes that the term "electronic will" actually encompasses three separate categories of wills that involve electronic media: The first category is offline electronic wills, which are written and stored locally on the testator's computer or other device.[70] For example, imagine someone writing her will in a Word document and storing it on her laptop. The second category is online electronic wills, where a will is created or stored through a third party.[71] For example, imagine someone writing her will in a Facebook message to a friend. Finally, the third category is qualified custodian electronic wills, where a "for-profit entity undertakes to become a 'qualified custodian' that would create, execute, and store the testator's will, subject to rules and regulations put forth by a state."[72] For example, imagine someone creating her will using the website of a start-up that markets its services in assisting with wills. Each category of electronic wills poses a unique set of challenges under current will formality requirements. The Chapter addresses the issues inherent to offline electronic wills,[73] online electronic wills,[74] and qualified custodian electronic wills[75] in turn, highlighting tensions between each of these categories and the purpose of will formalities. In its conclusion, the Chapter anticipates the continuing rise of electronic wills, encouraging scholars and courts to develop a systematic method of analyzing such wills under the traditional formalities.[76]

Together, the four Chapters of this issue of *Developments in the Law* highlight the challenges that go hand-in-hand with the rise of internet and computer use. By storing so much of our personal data online, we have created novel legal issues related to law enforcement, national security, privacy, and even donative transfers. These Chapters seek to shed some light on these new legal issues and suggest ways in which the law can adapt to our new reality.

---

[67] *Id.* at 1792–93.
[68] *Id.* at 1793–95.
[69] *Id.* at 1795–96.
[70] *Id.* at 1796.
[71] *Id.* at 1801–02.
[72] *Id.* at 1806.
[73] *Id.* at 1797–801.
[74] *Id.* at 1801–06.
[75] *Id.* at 1806–09.
[76] *Id.* at 1809–11.