The New York Review of Books

Private Eyes

Sue Halpern

March 9, 2023 issue

The surveillance economy has all but eliminated Americans' ability to be "let alone."

The Heads of State

Illustration by Jason Kernevich

Reviewed:

The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age
by Danielle Keats Citron
Norton, 291 pp., $30.00

Seek and Hide: The Tangled History of the Right to Privacy
by Amy Gajda
Viking, 376 pp., $30.00

In the fall of 2020, images of a woman using the toilet in her own home, taken by a Roomba robotic vacuum cleaner, began circulating on Facebook. How they ended up on the social media site was not surprising: someone with access to the company's data files had leaked them. How that person came to possess them also was not remarkable: Roomba was having some of its vacuum cleaners take photographs as they roamed through customers' homes in order to "train" the machines' artificial intelligence systems to recognize furniture and cats and dog bowls and other objects of daily living. But since vacuum cleaners can't train themselves (yet), the images needed actual humans to identify and label those objects, and it appears that one of the workers who came across the photos of the woman in her bathroom took the liberty of sharing them. According to a spokesperson for Roomba, the woman—and others using the vacuums—had consented to having them snap random photos inside their homes. But it is highly unlikely that those consumers also consented to having images of their home life posted and shared on Facebook.*

By Internet standards, the toilet photos are tame. They are also not uncommon. The online universe is full of easily accessible images of people—typically women—unaware that their bodies and intimate moments have been captured and broadcast for someone else's entertainment. Indeed, it is possible to read *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age*, Danielle Citron's powerful argument for laws to protect "intimate privacy"—which she defines as "the social norms (attitudes, expectations, and behaviors) that set and fortify the boundaries around our intimate lives"—as a disturbing catalog of the many ways humans are using digital technology to humiliate, expose, and coerce others.

In *The Fight for Privacy* she writes, for example, of South Korea, where cameras hidden in hair-dryer holders, wall sockets, and television sets secretly filmed 1,600 guests at forty-two motels. She points to China, where it is not unusual for men to take "up-skirt" photos of women, and to Australia, which saw a 249 percent increase in nonconsensual pornography in the midst of the Covid pandemic. Citron is a law professor at the University of Virginia, a MacArthur Fellow, and the vice-president of the Cyber Civil Rights Initiative, which advocates against online abuse. Her book is a reminder that our bodies, especially the bodies of women and girls, have become fair game for all kinds of online offenses, and that our most private behaviors, desires, and relationships can be exploited using digital media.

It would be simple—and not wholly wrong—to blame advances in technology for what appears to be the exponential rise in the number of these infringements. Certainly the proliferation of mobile phones and their apps, the expansion of artificial intelligence, the popularity of social media, and the sheer scale of the Internet itself have made it easy to create or acquire, and then disseminate, images like the ones taken by the Roomba. There could not be deepfake videos—which

insert faces and/or words into compromising media or, as *The New York Times* recently reported, enable realistic-looking, AI-generated people (in that case, "newscasters") to spread propaganda and falsehoods—without the software to make those videos, and they would not have the reach they do without the Internet. Citron notes that of the 50,000 deepfake videos posted in 2020, "about 95% inserted women's faces into porn." Once images and videos begin circulating online, it is often impossible to remove them.

But technologies are human inventions, and the ones that are used to violate private spaces and personal lives require human agency. A person had to decide to steal the Roomba photos and then leak them. A deepfake video does not create itself. Nor do up-skirt photos. An increase in nonconsensual pornography websites, from forty in 2013 to 9,500 in 2020, is not inadvertent. People—motivated by revenge, money, kicks, and all manner of moral turpitude—are responsible for co-opting digital technology. And in many ways, particularly in the United States, they are abetted by the law, or by the absence of legal penalties.

There is no explicit constitutional right to privacy in American jurisprudence. At best, privacy is protected by a hodgepodge of common law findings as well as by protections embedded in the First, Third, Fourth, Fifth, and Ninth Amendments of the Bill of Rights. The latter form what the Supreme Court, in *Griswold* v. *Connecticut* (1965) —which allowed married couples to purchase contraceptives—called a "penumbra" of privacy. Tort law has also been used to assert privacy claims, since some torts, such as misappropriation of one's image or identity and the publication of private facts that portray someone in a "false light," are meant to protect an individual's sovereignty and reputation. But in no case is a right to privacy settled law.

It was not until 1890, in a *Harvard Law Review* article entitled "The Right to Privacy" by the Boston lawyer Samuel Warren and his law partner, the future Supreme Court justice Louis Brandeis, that privacy was proposed as a jurisprudential imperative. In 1916 the legal scholar Roscoe Pound said that the article did "nothing less than [add] a chapter to our law." Citron, for her part, calls it the "foundation of American privacy law." In it, the two men lay out the case for the "right to be let alone," away from the prying eyes of photographers, journalists, and a prurient public. As Citron tells it, Warren was keen to protect his homosexual brother—and by association his prominent, wealthy family—from gossip columnists and others inclined to expose the details of his romantic life. Brandeis and Warren were also concerned that the new technology of photography was infiltrating private spaces and exposing its subjects to obnoxious scrutiny. They wrote:

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

Though Warren and Brandeis were arguing that the law should recognize a previously unarticulated right to privacy, they marshaled existing laws and precedent to do so, and privacy claims in courts and in the court of public opinion predate their article. As Amy Gajda, a professor at Tulane Law School and a former journalist, observes in *Seek and Hide: The Tangled History of the Right to Privacy*, that history often involved efforts by prominent men to block their peccadilloes from being aired in public. Gajda, who is a deft storyteller, recounts the machinations of Alexander Hamilton, Thomas Jefferson, and Grover Cleveland, among many others, to keep their private lives out of the press; Jefferson was so eager to preserve his privacy that he wrote his personal correspondence in code. In almost every instance—then and today—the cases reveal a tension between journalists' insistence that the public has a right to know about the character of people in public life and the countervailing belief, held by those public people, that their status does not make them any less deserving of an unscrutinized private life.

This tension persists, and the balance seesaws in one direction or the other depending on the social and political norms of an era. As citizens, we may have an instinctive affinity for laws that preserve our own privacy, but we also look to the press to expose the lies and hypocrisies of the powerful. As Warren and Brandeis saw it:

> Peculiarities of manner and person, which in the ordinary individual should be free from comment, may acquire a public importance, if found in a candidate for political office. Some further discrimination is necessary, therefore, than to class facts or deeds as public or private according to a standard to be applied to the fact or deed *per se*. To publish of a modest and retiring individual that he suffers from an impediment in his speech or that he cannot spell correctly, is an unwarranted, if not an unexampled, infringement of his rights, while to state and comment on the same characteristics found in a would-be congressman could not be regarded as beyond the pale of propriety.

Still, the effort to distinguish between private and public citizens can be fraught. Do we need to know, for example, that someone who teaches elementary school during the week is a drag queen on the weekends? Some parents (as well as, say, evangelical Christians and QAnon adherents) might think so; the rest of us might not. Conversely, is it the obligation of the press to "out" a senator who votes against gay rights but is known to hire male escorts and frequent leather bars, when that senator wants to keep his sexual identity hidden? A dogmatic belief in the primacy of privacy over publicity, Gajda cautions, can be appropriated by the powerful to operate outside of public view, which in turn can reinforce their power. (Not surprisingly,

she cites Donald Trump's efforts to conceal his tax returns.) What distinguishes the digital age we now inhabit is that anyone with a computer or a cell phone and access to the Internet can be a "publisher" simply by sharing things on social media and other sites (like Pornhub). And anyone, even children, can be the subject of their posts. The old, if porous, distinction between a prominent person and what Warren and Brandeis called "ordinary" individuals no longer applies.

In a sense, Warren and Brandeis anticipated this when they acknowledged the threat to privacy posed by photography and argued that it was imperative for the law to evolve as technology did. Nearly forty years later, in his dissent in *Olmstead* v. *United States* (1928), Brandeis recognized the threat to privacy of yet another new technology, wiretapping. In that case, law enforcement, operating without a warrant, listened in on the business dealings of a known bootlegger; the Supreme Court held, in a 5–4 decision, that this was not a violation of the recorded parties' Fourth and Fifth Amendment rights.

Brandeis disagreed. He argued that the Founders had "conferred, as against the government, the right to be let alone—the most comprehensive of rights, and the right most valued by civilized men." (It took another forty years before that decision was overturned by the Court.) More recently, the Court has decided that the police cannot search the contents of a suspect's cell phone without a warrant. But these are cases that address government overreach. When it comes to violations of intimate privacy by private individuals and website operators, victims are often stymied by the law itself in the form of a single statute—Section 230 of the Communications Decency Act of 1996.

A lot has been written about Section 230, much of it by Citron. The author of *Hate Crimes in Cyberspace* (2014), she recognized its dangers early on. The law, which exempts Internet platforms (such as Facebook or the dating app Grindr) from liability for material posted on their sites, was originally intended by its authors, the Republican congressman Chris Cox and the Democratic congressman Ron Wyden, to ensure that those platforms would be able to remove content that violated their terms of service or public sensibilities without being sued. It did this with these words: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The idea was that if they were not publishers, they would be able to avoid liability for

> any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected.

In practice, the courts have glommed on to the first part and skipped the rest. As a consequence, Internet platforms, in Citron's words, have been given "a free pass" to promote election disinformation, vaccine misinformation, so-called revenge porn, doctored photographs and videos, and other heinous material. (Sex trafficking and images that display evidence of child sexual abuse are the only content that is prohibited.) This has angered lawmakers on the left, who have called for Section 230 to be repealed. Remarkably, lawmakers on the right are also eager to see Section 230 scrapped, but for a different reason: they believe it enables websites to suppress and censor conservative points of view.

The Heads of State

Illustration by Jason Kernevich

In an opinion piece published in *The Wall Street Journal* recently with the headline "Republicans and Democrats, Unite Against Big Tech Abuses," President Joe Biden, seizing on one of the few issues that have bipartisan congressional support, called on lawmakers to finally reform Section 230. But so far, all efforts to fix or abolish it have failed, because Section 230 is crucial to the bottom lines of companies like Facebook and Google, whose armies of lobbyists work hard to ensure that it remains on the books. Meanwhile, Section 230 has now been exported to Canada and Mexico through trade agreements, so that citizens of those countries, too, will not be able to hold Internet companies liable for egregious content on their sites. The Supreme Court is poised to rule on two Section 230 cases later this year.

When Cox and Wyden proposed Section 230, they were aiming to create space for the fledgling Internet to grow and flourish. They did not anticipate that it would instead promote harmful, threatening, and vile content. Similarly the public at large, enamored of the new phenomenon of the Internet, was largely blind, and then indifferent, to the consequences of trading access to their personal viewing habits in exchange for the opportunity to use online services where they would be "served" ads. While the bits of data collected from any one interaction may be inconsequential (though not, of course, if they reveal something personal that one might not want shared, such as a cancer diagnosis or a predilection for BDSM), in the aggregate they have spawned a multibillion-dollar data brokerage industry that seemingly knows more about us than we do about ourselves.

This has been exacerbated by the Internet of Things, which has introduced all sorts of "smart" appliances into our homes that are collecting data on our activities, and Internet-connected wearable devices like sleep monitors and sport watches. A sex toy company called We-Vibe, for instance, obtains and stores data on when, how often, and at what speed individuals use its vibrators. Smart speakers like Amazon's Alexa record, store, and share private conversations with the company. Apple's virtual assistant, Siri, has been known to record (and send back to the company) the sounds of people having sex.

Pharmacies sell their customers' prescription information to data brokers; those data brokers know who has HIV and who has searched the Internet for abortion services. (That information may be used to take legal action against people in states with the most restrictive abortion laws.) Citron writes about how pregnant women on public assistance are often required by state Medicaid rules to provide reams of private information, such as their histories of sexual assault, abortion, and drug use:

> Even if they don't seek public assistance for prenatal care, they will be subject to government surveillance. If women come to a public hospital for delivery without having received prenatal care, then the hospital will likely hold the infant until the state inspects the woman's home and finds her competent to raise her child.

The surveillance economy that has grown up around the Internet and the free pass given to companies that run social media and other web-based platforms have dramatically curtailed the possibility of being "let alone," even in our offline lives, where our behaviors are still being monitored and our personal data continues to be collected. (This is in the United States; the European Union has much more stringent rules and regulations, including the right to be forgotten in Internet search databases if they call up personal information that serves no public purpose.) As Citron shows in example after example,

there are few, if any, remedies for people whose lives have been upended by false, misleading, compromising, or threatening words and images circulating on the Internet. So what is to be done?

Citron, who calls herself a bit of a Pollyanna, has many ideas for how to protect our personal lives from online sabotage, some of which might also curb the excesses of the surveillance economy, which she calls "Spying Inc." The most practicable is a proposal for revising—rather than eliminating—Section 230:

> Congress should amend Section 230 to make clear that platforms and search engines can be sued for injunctive relief in the form of deleting, blocking, or de-linking intimate images that have been published without written consent.

This amendment, she says, "should allow plaintiffs to recover attorney's fees," which would have the ancillary effect of encouraging more lawyers to take on these cases.

Concurrently, Citron proposes that the statute preserve website owners' immunity from prosecution if they can show that they have taken "reasonable" steps to remove the offensive content. What is "reasonable" is left up to the courts (whose interpretation of Section 230 has historically favored the tech companies) and, Citron believes, should not be adjudicated on the basis of "whether the platform acted reasonably in a specific case, but rather if, as a general matter, it had been acting reasonably to address the type of illegality at issue." In this way, she says, companies would feel compelled to adopt more robust content moderation.

This, of course, is speculative, but it is true that provisions in the European Union's General Data Protection Regulation (GDPR), and the more stringent data laws on the books in states like California and Illinois, have pushed tech companies to behave more responsibly—or at least to appear to do so. (You can thank the GDPR for being asked, each time you visit a website, if you will accept all its cookies, where "cookie" is a euphemism for "tracker.") A comprehensive federal privacy law, which Citron lays out in great and somewhat technical detail, would go a long way toward requiring companies to do the right thing. (In his *Wall Street Journal* piece, Biden tiptoes into this territory, calling for "serious federal protections.")

Citron's most radical—and most aspirational—idea, and the one that is central to her thinking, is for what she calls "intimate privacy" to be considered, by law, a civil right, "understood as both a basic entitlement and an antidiscrimination mandate." If it were, she argues, that would "clarify [its] moral significance." It would also

> give us the vocabulary to understand its centrality to the development of an authentic and dignified identity. It would signal that intimate privacy is a precondition to love, friendship, and civic engagement. It would convey the necessity of intimate privacy for individual *and* community development. It would communicate to Spying Inc. that intimate privacy deserves strong protections, rather than empty gestures.

It's an appealing idea, but short of an act of Congress, it's unclear how intimate privacy could be folded into civil rights law, especially now that Republican lawmakers and a deeply conservative Supreme Court appear to have little interest in protecting the civil rights that are currently on the books. Meanwhile in states across the country, the right wing has been actively passing laws to police citizens' private lives, in some states, notably Texas and Oklahoma, deputizing citizens to spy on each other, with the promise of a bounty for doing so. Indeed, privacy has never seemed more contested, and more out of reach.

That sentiment, Gajda observes in *Seek and Hide*, is historically consistent. "We may think that we've never needed the right to privacy as much as we do today," she writes. "But that's what nearly every generation before us has thought too." This time, though, it may be true.

Sue Halpern

Sue Halpern is a staff writer at *The New Yorker* and a regular contributor to *The New York Review*. She is a Scholar in Residence at Middlebury. (March 2023)

* See Eileen Guo, "A Roomba Recorded a Woman on the Toilet. How Did Screenshots End Up on Facebook?," *MIT Technology Review*, December 19, 2022. ↩