Introduction

WE ARE LIVING IN A CHILLING NEW ERA

It was a bright cold day in April, and each of these stories was in the news: An American permanent resident, who possesses many of the same legal and constitutional rights of citizens – including freedom of speech – is detained and rendered to a secret facility by United States federal authorities for promoting and engaging in university campus protests – activities all protected by the US Constitution.[1] A member of Congress calls for the Federal Bureau of Investigation (FBI) and Department of Justice to criminally investigate protests at retail locations for a business owned by one of the world's most wealthy and powerful men – a titan of the technology industry who is now also a controversial and powerful White House official – in many ways, a "shadow" president in Donald Trump's new administration.[2] A US attorney based in Washington, DC sends target letters threatening to prosecute anyone that "obstructs" the work of a secretive government agency that has been systematically dismantling critical government infrastructure, including the administration of social security, health, and nuclear management.[3] Private sector data contractors are conducting large-scale online surveillance to help government authorities map and track a person's "activity, movements, and relationships."[4] And as most social media companies increasingly engage in vast surveillance for profit,[5] others like X (formerly known as Twitter) – one of the most popular social media platforms in the world, and now owned by that same powerful White House official – have been transformed into massive pro-government propaganda machines, where lies, disinformation, harassment, abuse, and hate are not just rampant but amplified.[6]

What links each of these cases is not just that they all happened within the same few weeks, but the fact they are all examples of government, commercial enterprise, and technology being intentionally wielded to create a profound *chilling effect* on people's fundamental rights and freedoms.[7] By "chilling effect," I meant just as the words suggest – a cooling or inhibiting effect where people are deterred or discouraged from speaking or acting freely due to some threat – like the threat of surveillance or prosecution by federal authorities or threats of violence and harassment by

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

malicious actors on social media. These cases are not comprehensive. They are a mere sample of the many ways state, corporate, and technological power is presently being weaponized in unprecedented ways to chill and repress us.

How did we get here? It is impossible to create a precise road map for this chilling new era and when it began, though there have been important milestones. Edward Snowden's revelations about mass government surveillance were undoubtedly a critical early one. Though over a decade ago, most privacy lawyers and scholars still remember where they were when stories about Snowden's national security leaks first broke. The former National Security Agency (NSA) contractor had exposed to the world a trove of classified US Government documents disclosing the existence of highly secretive and extensive mass surveillance programs being used by US intelligence agencies and their partners in the West.[8] Starting in June 2013, the *Guardian* and *Washington Post* would publish a series of stories detailing these top- secret surveillance tools and programs. There was the PRISM surveillance program, which involved the NSA and FBI tapping directly into the main servers of nine leading US internet and social media companies – Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple – and extracting audio and video data, chat logs, images, emails, and other documents to track targets.[9] There was the NSA surveillance tool XKEYSCORE, which allowed the agency to collect, analyze, and probe massive troves of online content and metadata concerning "nearly everything a user does on the internet."[10] There was ECHELON, a global surveillance collaboration between the US, Canada, the United Kingdom, Australia, and New Zealand involving tapping into digital telecommunications with intercept stations around the world.[11] It was as if the dystopian futures of total surveillance, manipulation, and control envisioned in George Orwell's *Nineteen Eighty-Four*[12] or Aldous Huxley's *Brave New World*[13] were no long mere visions, but our lived reality; except it wasn't just big government behind it all, but big business – especially big tech.[14] It was shocking, at least at the time. In retrospect, the national security surveillance programs disclosed by Snowden arguably pale in comparison to the Trump administration's more recent use and abuse of law, surveillance, and technology to chill and repress.

Nevertheless, I remember where I was that June – in my small shared apartment in Cambridge, Massachusetts, and in the process of packing my bags. I was nearing the end of a fellowship at Harvard's Berkman Klein Center for Internet & Society, a research center that's been at the forefront of technology law and policy issues for decades – including privacy, a key focal point of my research. My plan had been to soon return to Oxford University, where I was then still a doctoral student. As I read about the fascinating but deeply troubling revelations about mass online government surveillance contained in the Snowden leaks, certain questions were burning in my mind: How would this surveillance impact on people's behavior? Would it have a *chilling effect* on people's rights and freedoms in the US and around the world? I had been wrestling with similar questions in my doctoral work at Oxford, but now the Snowden revelations had created a unique opportunity to study the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

questions in real time. I would not have to design an experiment to carry out in some cloistered university lab. We were all living in a mass surveillance experiment now.

In research that began at Harvard that spring and continued at Oxford the following year, I would conduct a study to answer these very questions – by exploring the impact these NSA surveillance programs had on people's use of Wikipedia, the immensely popular online encyclopedia. I was not prepared for what I would find: clear and compelling evidence of chilling effects due to the threat of NSA surveillance, whereby tens of millions of people, maybe more, were being chilled from freely searching and informing themselves online.[15] My study, which I will talk about in more detail in Chapter 1, would be among the very first in the world to document real world chilling effects caused by mass surveillance.[16] My findings would receive extensive media coverage in the US and around the world. When I began fielding media calls and emails not just from the United States or Canada, but from places as far flung as India, Russia, South Korea, and New Zealand, it became clear how the findings had struck a deeper, even universal chord: people were deeply worried and troubled about online surveillance and its impacts *everywhere*.

As the widespread coverage and international interest suggested, my study offered compelling insight as to what is at stake in the threat chilling effects pose to human rights and democracy, both today and tomorrow. For that reason, the study would also thrust me into the middle of high stakes litigation between the Wikimedia Foundation – the nonprofit organization that runs Wikipedia – and the US Government after lawyers for the Wikimedia Foundation and the American Civil Liberties Union (ACLU) asked me to act as an expert witness in support of their lawsuit. I did so *pro bono* because I believed in the importance of the rights at stake.[17] On the day that the lawsuit was filed just a few years later, a case that challenged the constitutionality of various NSA surveillance programs, Wikipedia founder Jimmy Wales and Wikimedia Foundation Executive Director Lila Tretikov would write in an op-ed in the *New York Times*:

> The notion that the N.S.A. is monitoring Wikipedia's users is not, unfortunately, a stretch of the imagination. One of the documents revealed by the whistle-blower Edward J. Snowden specifically identified Wikipedia as a target for surveillance, alongside several other major websites like CNN.com, Gmail and Facebook. The leaked slide from a classified PowerPoint presentation declared that monitoring these sites could allow N.S.A. analysts to learn "nearly everything a typical user does on the Internet."
>
> The harm to Wikimedia and the hundreds of millions of people who visit our websites is clear: Pervasive surveillance has a chilling effect. It stifles freedom of expression and the free exchange of knowledge that Wikimedia was designed to enable.[18]

Indeed, if people are chilled from seeking out information, freely reading, and informing themselves on sensitive and contentious matters of public policy like

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

terrorism and national security, that is deeply corrosive to freedom and democracy. Their lawsuit – *Wikimedia Foundation v. NSA* – remains ongoing. But in the decade since the Snowden leaks, the threats did not subside, but only grew in size and scope.

GROWING THREATS

With the Snowden revelations still fresh in memory, *The Guardian* and the *New York Times* would break another explosive surveillance and data-tracking story just a few years later in March 2018. This one involved a murky and now infamous British political consulting and data science firm called Cambridge Analytica and the social media giant Facebook.[19] Cambridge Analytica had inappropriately harvested data from the Facebook profiles of more than 87 million people – collecting and retaining profile pictures, posts, comments, personal preferences, group memberships, any and all personal information data it could access – the vast majority of whom had not consented to even the firm's access to the data, let alone how it would be ultimately used. Cambridge Analytica used that misappropriated data to build "psychographic profiles" of voters to target them with tailored ads, messaging, and other influence operations both to help Donald Trump's campaign in the 2016 US presidential election and pro-Brexit groups in the United Kingdom's referendum on European Union membership that same year.

Not surprisingly, like the mass government surveillance that I explored in my own Wikipedia study, the large-scale corporate surveillance and data-mining operation in the Cambridge Analytica scandal also had substantial chilling effects. In a study of over 2,200 American social media users a few months later, researchers found that 42 percent of these users reported that the Cambridge Analytica scandal had caused them to change their behavior on Facebook, including 25 percent self-censoring their posts; 19 percent posting less; 19 percent changing privacy settings; and another 10 percent deleting or deactivating their accounts.[20] Another 26 percent in the study indicated that the Cambridge Analytica scandal had caused them to change their behavior on "other social media," including 20 percent being more careful about what they post; 12 percent posting less; and 4 percent deactivating or deleting their accounts. Furthermore, 39 percent indicated that their posting and sharing on social media was "way less personal." Overall, 79 percent said they were "very" or "somewhat" concerned about the privacy of their information on social media, and 82 percent said they self-censor on social media due to privacy concerns. *The Atlantic*, reporting the findings, observed that "people are changing the way they use social media," including being far less personal in their posting online, and the privacy invasions of scandals like Cambridge Analytica were likely to blame.[21]

Less than two years later, the *New York Times* would break a story about another shadowy company – one that may, the *Times* predicted, "end privacy as we know it."[22]

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

That company, Clearview AI, had developed a revolutionary facial recognition technology (FRT) application powered by cutting-edge artificial intelligence (AI) and machine learning capabilities. It claimed that it could identify anyone based on a single photo or image with astonishing accuracy that no other facial recognition software could match: a 98.6 percent accuracy rate.[23] Perhaps the best measure of its capabilities has been the company's success – thousands of police services around the world have used it, and many more are eager to try.[24] Kashmir Hill, the journalist who would ultimately break the story about Clearview AI for the *Times*¸ was originally skeptical but later convinced through countless demonstrations and by using the tool herself of its immense capabilities – and immense threat to privacy and potential for chilling effects.[25] But what was chilling about Clearview AI wasn't *just* the powerful AI-driven facial recognition surveillance system it was secretly marketing to law enforcement around the world, but *how* it developed that technology. As it turns out, the company trained the AI powering its surveillance system using billions of facial images it illegally "scraped" – extracted at scale using automated programs – from social media platforms like Facebook, Instagram, and LinkedIn.[26] If the surveillance, facial identification, and tracking capabilities that Clearview AI touts sound dystopian and far-fetched, like something right out of those same science fiction novels, they are equaled only by its creepy and villainous origin story: a deeply chilling surveillance technology developed through mass global privacy violations. That brings to mind science fiction like Mary Shelley's *Frankenstein* as much as Orwell's *Nineteen Eighty-Four*. Yet, the threat to privacy – and potential for widespread societal chilling effects – posed by a new generation of companies like Clearview AI, using and abusing AI, FRT, and other emerging technologies for profit, was very real.

Take the story of Derrick Ingram. Ingram, a 28-year-old Black Lives Matter activist living in New York City, found himself barricaded in his Hell's Kitchen apartment in the early hours of August 7, 2020, surrounded by dozens of officers from the New York Police Department (NYPD).[27] The officers claimed they had a warrant for his arrest – supposedly based on his use of a megaphone at a protest months earlier.[28] While Ingram frantically consulted with various public defender lawyers on the phone as he live-streamed the encounter, he could hear police drones buzzing overhead. In the end, Ingram was not arrested and though charges were later filed against him, those charges were also eventually dismissed. But what was just as troubling as the stark show of police force that day, was how police had located him. It turns out that video of the police standoff showed officers outside his home reviewing a document entitled *Facial Identification Section Informational Lead Report*, which included a photo of Ingram from his own publicly accessible Instagram account.[29] That photo, which captured a clear image of his face, was taken at a bar following a protest and posted the same day – August 6, 2020 – the day before the police standoff at his home. In fact, the NYPD would later confirm that it used FRT in its investigation but would not provide any more details.[30] But it seems improbable that the

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

photo did not play a role, given the timing. A later report by *BuzzFeed* would confirm that the NYPD had contracted the services of Clearview AI at the time.[31]

The ongoing threats of police investigations, rearrest, and targeted surveillance have chilled Ingram's activism and his life. He has moderated his social justice protesting and campaigning and now describes himself as far less "reactionary."[32] He has withdrawn from social events and also declined work opportunities, including what he described as a "dream job" offer, just because he was still struggling psychologically with these threats, and believed he would fail if he took on the work.[33] "People know my address now … I'm scared every day, but I don't have the means to relocate," Ingram has said.[34] Clearview AI had boasted it could identify a person with a single photo. It appeared to have helped the NYPD do so with Ingram. The threat and chilling effects were real and profound.

And it's not just individuals or activists who are impacted. It is entire communities. Like the border town of Chula Vista, California, where poorer immigrant communities find themselves in the flight path of the town's growing fleet of drones.[35] In October 2018, Chula Vista became the first city in the US to launch a "Drone as First Responder" program, wherein 911 dispatchers can send drones as first responders to deal with emergencies, including crimes in progress and other threats to public safety.[36] Since then, drones have flown 20,000 times in the town. While some residents support the drone program, others report impacts that suggest broader chilling effects due to the privacy threats. Some residents report they feel "constantly watched."[37] Others report being afraid to use their backyards or other public spaces out of fear they are under surveillance. Another resident reports suffering persistent anxiety and sleep deprivation.[38] And these chilling effects are not endured uniformly, but impact certain communities more than others. *WIRED* magazine analyzed data for the drone flights and found a pattern: the poorer the neighborhood, the more it is exposed to drones.[39] Those poorer neighborhoods tend to be populated by working class black, Hispanic, and immigrant populations.[40] Those living homeless in the town report feeling as if they live in a "surveillance dystopia," as drones regularly fly low over their encampments.[41] In a drone town, a lack of a home means no privacy and thus no relief. In other words, the drone surveillance is impacting the entire town, but these resulting chilling effects disproportionately impact poor, working class, and racial communities. These differential impacts are another reality of chilling effects.

Nor is it only overreaching government, law enforcement, or commercial enterprise contributing to the problem. New technologies are also enabling abusers, who chill victims through targeted threats, stalking, harassment, and cyber-mobs. And the victims of these threats are disproportionately women and racial and sexual minorities.[42] Take the story of Stephanie Feldman, a novelist and editor. Feldman was at work when she first learned someone had stolen her online identity and had launched a persistent online harassment campaign that would chill her, and her friends and colleagues, with impacts that still affect her life today.[43] The perpetrator

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

had created a Twitter account – the social media platform now known as X – to impersonate her using only a photo and a login, nothing more. The perpetrator proceeded to portray Feldman as a feminist who supported "white genocide" – killing all white males – that inevitably unleashed a campaign of threats, harassment, and abuse from a virtual cyber-mob directed toward Feldman herself.[44] The attacker also went after her publisher and employer, trying to get her fired.[45] For months after the attack, Feldman received daily threats and hate mail that caused her to fear for her safety. She began to self-censor both her writing and online communications and withdrew from social media and the internet altogether.[46] She even became too fearful to promote a new book that she had edited online, afraid it would lead to further attacks on her or the writers that contributed to it.[47] In some US states, laws like the Texas Heartbeat Act are being specifically designed to weaponize chilling effects to eviscerate even constitutionally protected rights by outsourcing to private parties not just legal prosecution, but also targeted stalking and harassment campaigns just like this.[48] Like Feldman, victims of such state-directed or supported campaigns of stalking and harassment are not only chilled from speaking or exercising their rights, but living.

None of this is coincidental. Today, surveillance and censorship is on the rise everywhere.[49] More data is being collected, analyzed, mined, and stored about us and our daily activities than at any other time in history.[50] We now speak of "big data" – massive data sets generated from billions of daily online transactions; emails; texts; digital media; searches; comments; likes; posts; health records; social media activities; streaming services; scientific data; GPS trackers; smart phones; smart appliances; and new surveillance and sensory technology, among many other things.[51] These data sets are larger, more varied, and more complex than at any other time in history.[52] For instance, by 2003 all human activity in history had created a total of five exabytes (10^{18} bytes) of data. As of 2013, that amount was being generated every two days. Today, big data is even bigger – every day, the internet alone processes 1,826 petabytes of data; Google processes 3.5 billion searches; Facebook users upload 300 million photos and make over 500,000 comments and nearly 300,000 status updates.[53] Advanced new data-mining techniques, enabled by AI, machine learning, and automation, have been developed to analyze and excavate these massive data sets to predict and influence our behavior to advance both state and corporate interests.[54] These same advanced technologies and techniques are being used in astonishing and disturbing new ways to analyze and employ data to track, censor, manipulate, and control us,[55] automate legal and regulatory enforcement,[56] or to promote corporate interests.[57] Meanwhile, ubiquitous computing, social media use, and the internet of things, have made targeted spying, stalking, harassment, and cyber-mobbing not only easier, but far too common.[58]

Not surprisingly, concerns about the impact of these developments on privacy, speech, and other fundamental rights and freedoms – particularly their chilling effects on these rights and freedoms – have taken on greater urgency and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

importance.[59] Indeed, beyond law and social science, the term "chilling effects" has taken hold in "everyday discourse."[60] And the COVID-19 pandemic – resulting in citizen health tracking and surveillance infrastructure – and sweeping recent legal changes – like the widespread criminalization and restriction of abortion and other reproductive freedoms following the US Supreme Court's decision in *Dobbs* – have only compounded these chilling effect concerns.[61] Thus the scale of impact is likely far broader than individuals, groups, or even communities, affecting entire populations – as my research on the chilling effects of government surveillance on Wikipedia use has shown. Even those fortunate enough to escape repressive or authoritarian regimes abroad are no longer safe. For instance, my colleagues at The Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto – where I have been a long-term research fellow – have extensively documented how authoritarian governments are increasingly engaging in forms of transnational campaigns of targeted surveillance, stalking, and harassment to chill the speech and activism of dissidents and diaspora communities.[62] Chilling effects are local, and global.

A LONG HISTORY

Yet, these concerns about chilling effects are certainly not new, nor is overreach by government, commercial enterprise, and abusers in weaponizing chilling effects to repress and victimize. Modern history is littered with examples. Between 1917 and 1921, two-thirds of US states enacted intentionally vague and broadly construed anti-sedition laws in order to criminalize and chill the speech and activities of labor unions and the broader labor movement.[63] During the "red scare" of the McCarthy era – which I will talk about in more depth in Chapter 1 – in addition to states passing repressive, vague, and overreaching anti-communist statutes to chill left-wing groups and their activities, state and federal authorities also targeted them with persistent surveillance and regularly released publicly lists of alleged communists and socialists. The aim was to weaponize employers and the general public into blacklisting, firing, and socially punishing those named, to create a broader climate of fear and chilling effects.[64] As historian Lawrence Cappello has observed, all of these vague laws, surveillance, and tactics to create vast chilling effects were later repurposed in the 1950s and 1960s to victimize and chill the civil rights movement, and later saw use in the Watergate scandals of the 1970s, Iran-Contra of the 1980s, and the overreach of national security surveillance and law enforcement in the early twenty-first century following the 9/11 terrorist attacks.[65]

To be clear, while many of these examples highlight governments and police weaponizing chill, corporate actors have long done so too. There is also a long history of companies using legal threats to chill and deter critics.[66] For instance, "SLAPP" lawsuits are an explicit example of this. The term "SLAPP suits" – Strategic Lawsuits Against Public Participation – was coined by two University of Denver professors in

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

the 1980s to refer to lawsuits threatened or filed by companies to chill people from speaking publicly on matters in the public interest – something they observed among large construction companies that regularly threatened citizens and activists who publicly criticized them for environmental abuses.[67] SLAPP suits are an explicit case of chilling effects being weaponized to preserve or extend corporate power, with perpetrators usually powerful companies or business persons who use them to suppress news reporting or to silence people who wish to speak out on corporate corruption, criminality, and other wrongdoing. The researchers documented tens of thousands of such cases in the US, but surely the number is even greater today, as SLAPP suits are now a global problem.[68] Similar legal threats have been employed by companies in many other contexts. For instance, Big Tobacco used persistent threats to chill government efforts to regulate or ban tobacco products,[69] while pharmaceutical companies have also been prolific in their legal threats to chill those who support industry regulation.[70] Businesses are also often complicit when governments weaponize chill to repress and control. State abuses were regularly carried out with private sector collaborators during the McCarthy, Civil Rights, and Watergate Eras.[71] And the antiabortion movement has a long history of weaponizing violence and violent threats to chill abortion access often enabled by corporate complicity or silence.[72]

This long history continues to unfold today. The Snowden leaks, Cambridge Analytica, and Clearview AI stories all involved similar joint ventures between powerful technology companies working closely with governments – what Bruce Schneier calls the surveillance-industrial complex[73] – to likewise enable more invasive mass surveillance and thus wider chilling effects. And as the stories recounted at the outset of this chapter suggest, we are likely at the dawn of an even more dangerous period where law, surveillance, and many other forms of state, technology, and corporate power are merged and weaponized to achieve society-wide chilling effects.[74] For instance, as I write, the second Trump administration, with the help of Elon Musk and other technology industry titans, is wielding technology in systematic and surprising new ways to monitor, influence, and repress. Overreaching new laws are being enacted across the US and around the world to chill the speech, reproductive freedoms, and other fundamental rights of women and sexual minorities,[75] while corporate actors secretly fund these efforts.[76] And right wing activists use online platforms to launch angry cyber-mobs to "doxx" (disclose their names, location, and other personal information), harass, stalk, threaten, and abuse them.[77] Feldman is an example of that kind of weaponized chill, which aims not only to obliterate people's rights, but chill and repress already marginalized and disempowered people and communities.

PERSISTENT SKEPTICISM

Yet even as concerns about chilling effects today grow, and there is increasing recognition that chilling effects are destructive to freedom and democracy, widespread

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

skepticism persists about their existence and impact. Though the idea of "chilling effects" is not new – it has been a part of US constitutional law since the Second World War – lawyers, legal scholars, privacy theorists, and social scientists often question whether chilling effects even exist, or if they do, whether their impacts are anything more than temporary, trivial, or ephemeral.[78] Skepticism among courts has persisted too, especially concerning chilling effects due to privacy threats like surveillance or personal threats like stalking and harassment. Judges tend to downplay, dismiss, or ignore such chilling effects entirely, or in other cases, create legal rules or barriers to make bringing claims based on such chilling effect concerns more difficult.[79] For example, in its 2013 decision in *Clapper v. Amnesty International*, the US Supreme Court dismissed chilling effects caused by government surveillance as "self-inflicted injuries" that were too "subjective" and "speculative."[80] And in its 2023 high-profile decision in *Counterman v. Colorado*,[81] the Court overturned a conviction under a Colorado anti-stalking law while entirely ignoring how the perpetrator's own stalking and harassment had had a profound chilling effect on the victim, a musician, causing her to live in constant fear of physical attack, cancel concerts, and ultimately abandon her singing career as a result.[82] Even in the high stakes litigation between the Wikimedia Foundation and the US Government in *Wikimedia Foundation v. NSA*,[83] in which I have been involved as an expert witness, the courts have been persistently dismissive of the lawsuit's claims of surveillance chilling effects as too speculative, despite compelling evidence of chilling effects. Such skepticism is not unique to American law. Lawyers, legal scholars, and judges in Canada, the United Kingdom, Europe, Australia, New Zealand, and beyond – nearly any jurisdiction that has recognized chilling effects in law and jurisprudence – have expressed similar skepticism.

Not only does skepticism persist, but how we conceptualize chilling effects is also a big problem. The conventional understanding is that a chilling effect is when a person, deterred by fear of some legal harm or punishment, engages in *self-censorship*, that is, censors themselves and does not speak or engage in some activity, despite that activity being lawful, even desirable.[84] This conventional focus on self-censorship and speech is not surprising – the idea of "chilling effects" first came to prominence in US constitutional law in a series of cases decided in the 1950s and 1960s, wherein the Court invoked the concept in striking down various overreaching McCarthy and Civil Rights Era laws for chilling First Amendment protected speech and other expressive activities.[85] And prominent First Amendment scholars – like Frederick Schauer, whose 1978 account of chilling effects is still today described as "definitive"[86] – have also helped explain and elaborate the Court's "chilling effects doctrine," which has tended to focus almost exclusively on legal and regulatory chilling effects and self-censorship: how vague and uncertain laws – and uncertainties inherent in the legal process – combined with the risk or threat of legal harms like criminal or civil penalties could chill First Amendment protected speech and behavior. Such law-centered claims are now widely recognized as First

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

Amendment injuries, with courts regularly invalidating statutes and regulations for having a chilling effect on First Amendment protected speech.[87] So, this understanding is predominant in US law as it's the conceptualization embraced by the US Supreme Court, as well as prominent legal scholars who have also adopted it and helped shape and define it. It is also predominant internationally, in many of those same countries noted earlier – wherever American law and jurisprudence has had influence.

Yet, this conventional conceptualization is too narrow, legalistic, and empirically weak, leaving us with little insight as to the *true* scope of chilling effects and their impacts and harms. It is too narrow because it focuses only on legalistic forms of chilling effects and thus cannot explain chilling effects in a range of other contexts – like those caused by surveillance or personal threats and abuse online. It is empirically weak as much of its assumptions about how and why people are chilled find little support in empirical evidence. And it neglects critical insights from a range of social science fields about how chilling effects involve not just an absence – self-censorship, which is a lack of speaking or doing – but also *shape* behavior. While self-censorship is an important dimension of chilling effects, it is only one dimension of the phenomena. In fact, chilling effects predominantly involve not just a deterrent effect, but a shaping effect – people speaking, acting, or doing in a way that conforms to, or is in compliance with, perceived norms, not simply self-censoring to avoid a legal harm. To borrow a term from Julie Cohen, chilling effects are also *productive*.[88] They not only involve the silencing of speech, but also the production of conforming and compliant speech and behavior. As such, this legalistic and unsupported conventional view cannot help us understand chilling effects and their true threat, and instead only feeds greater skepticism. That, in turn, makes it more difficult for victims to go to court to vindicate their rights in the face of invasive and repressive chilling effects due to surveillance and other targeted threats, and for policymakers to enact law reforms to address them.

Part of the problem is that there has been a significant dearth of theoretical and empirical studies of chilling effects, at least until recently. Legal scholars who were interested in the concept did not have the knowledge or training to do the empirical work necessary to study this behavioral phenomenon. And the social scientists who did have the training were less interested in chilling effects, given its legal origins and dimensions. Fortunately, that is changing. There is today a growing body of interdisciplinary research that theorizes and explores chilling effects not as a legal doctrine but as a behavioral phenomenon in a variety of contexts, like chilling effects due to government[89] and private sector surveillance,[90] data collection, processing, and profiling,[91] and targeted personal threats, harassment, and abuse.[92] The central focus of this new work – which should be recognized as an emerging but distinct field of interdisciplinary social scientific and legal inquiry – has moved on from the question of whether chilling effects exist to exploring and understanding them, and how to respond.[93] And what I argue in this book is that this new research,

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

when synthesized with insights from a variety of other fields of social and behavior science, shows that chilling effects are best understood as a powerful form of *conformity* and *compliance* effects with deeper psychological foundations. This theory builds on insights concerning the chilling effects of privacy and personal threats by scholars and theorists like Julie Cohen, Daniel Solove, Neil Richards, Margot Kaminski, Ryan Calo, Bruce Schneier, and Danielle Citron and links this behavioral phenomenon that lawyers have called "chilling effects" to a broader social and behavioral scientific literature on conformity and compliance and their evolutionary foundations.[94] And what this extensive body of behavioral theory and research tells us is that when facing certain perceived threats – like surveillance and observation; uncertainty about the law or other behavioral norms; or threats to personal safety – people do not act or speak freely but instead engage in self-censorship and conformity. That is, they act the way they believe others would act in the same circumstance or how they believe they are expected to act – they conform and comply.

So, chilling effects are a more powerful form of conformity and compliance effects. As we will see, people engage in behavioral conformity in response to personal threats for a variety of reasons. But a central one is for safety and security. There is strength in numbers. Conforming to the group, expected behavioral norms, or the expectations of broader society, ensures greater protection from threats, and reduces the risk of harm and likelihood of ostracism and alienation. This is also why conformity – and chilling effects – are a behavioral tendency with a deeper psychological foundation.[95] Throughout human history and evolution, those of us who engaged in conformity in response to threats were more likely to survive, because acting in compliance with norms of the group or community enhanced the likelihood of surviving the threat.[96] Breaking norms and behavioral expectations may leave you ostracized and alone – and more vulnerable to threats. Hence, this behavioral tendency has become hardwired into human psychology through evolutionary processes over a very long time. Thus, people can be chilled and engage in conformity and compliance both consciously and subconsciously. We often do it deliberately to avoid threats, but we also do it subconsciously – we can be chilled and we don't even know it.

What makes chilling effects *different* from garden variety social conformity is that they involve some of the most powerful kinds of threats. The central factors in a conformity theory of chilling effects tracks the central factors in conformity and compliance: observation; uncertainty; personalization; and power and authority. But when it comes to chilling effects, it is not merely observation by peers – that you find in psychology experiments exploring the conforming effects of mere observation – but systematic and persistent surveillance by powerful entities like government and law enforcement.[97] The uncertainty triggering chilling effects is often not simply uncertainty about behavioral norms, but uncertainty and ambiguity about legal requirements backed by significant criminal and civil penalties coupled with the threat of social ostracism and alienation associated with lawbreaking. The personal threats

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

are not just single threats of violence, but often large-scale campaigns of harassment, stalking, and intimate privacy violations, and abuse, sometimes enabled or directed by government itself.[98] In other words, chilling effects are a *more* powerful form of conformity and compliance that are magnified by the power and authority of government, law enforcement, and well-resourced commercial enterprise. Chilling effects are thus qualitatively and quantitatively different from typical forms of conformity and compliance due to the magnitude of threats at stake, but to understand them you must also understand conformity and compliance.

This *conformity* theory of chilling effects, which I explain and advance in this book, has a number of important theoretical, empirical, normative, and legal advantages. First, it is neither singular nor narrow, and unlike conventional theories focused on law or privacy alone, it is better grounded in social science and empirical literature. As such, it also has greater predictive and explanatory power. It offers a more comprehensive theory that better accounts for and explains chilling effects due to different kinds of threats.[99] And combined with insights from social and deterrence theory, it can predict the scope and magnitude of chilling effects in these different contexts too. Beyond more robust theoretical understanding, this also has important legal and public policy implications, including for chilling effects standing and doctrine. Second, it demonstrates more clearly how privacy and chilling effects theory are inextricably linked. If privacy theory is concerned with preserving social conditions for autonomy and self-development, then understanding chilling effects – which fosters competing social conditions favoring self-censorship, social conformity, and compliance – is essential.[100] Third, by theorizing chilling effects not just in relation to individual-level self-censorship but also broader social conditions and power dynamics, it provides a normative foundation to distinguish "good" and "bad" chilling effects, and also navigate competing ones – which also has implications for law and policy.

Most importantly, this theory of chilling effects helps us understand the far-reaching scale and scope of chilling effects, and how they are toxic and corrosive to democracy and civil society. It helps us understand how chilling effects deeply impact individuals – that we are wired, psychologically, to be chilled, and thus it can affect us even without our awareness. We are chilled into silence consciously, but also subconsciously. Chilling effects shape us, our psychology and personal identity, ultimately producing more docile people and populations that are easier to control. It helps us understand how these impacts are *compounding*, because that is also how conformity and compliance work. That is, as more threats are added, the chill becomes greater. This means that when a person is faced both by a surveillance threat, uncertainty, and personal threats, the chilling effect will necessarily be greater than a case where the person faces only one of these threats. It also helps us understand how chilling effects, and the threats that cause them, can help explain the increasing tribalism and extremism we see today, both online and offline. That's because conformity can sometimes encourage one to self-censor and

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

remain silent – behavior more often associated with chilling effects – if that is the expected norm. But it can also mean more polarizing and extreme speech or behavior, if that is the group norm that a person conforms with in the face of a threat. So, chilling effects can lead to both individual and even societal-scale censorship, but also more extremist behavior too.

Lastly, this theory better captures the broader social context of chilling effects and their relationship to existing social, economic, and political structures, power, and hierarchies, which is essential to understanding how chilling effects impact democratic societies. A behavioral phenomenon – caused by state and corporate actions – that encourages the production of speech and behavior that is more compliant and conforming has obvious implications in an era of surveillance capitalism and the emergence of mass citizen-tracking systems.

We need to change our thinking. We need to reject conventional approaches. We need to better understand chilling effects, the threats they pose, and what factors – like surveillance and other public and private sector actions – cause or magnify them. That is what this book is about – changing how we think about chilling effects so we are better prepared to stop them, and their corrosive impacts both on people and society. That's because a world rife with chilling effects – due to overreaching surveillance, targeted legal threats, vast algorithmic data collection and processing, and ubiquitous online threats and abuse fostered by big government and big business – is just as dystopian as the nightmarish totalitarian futures imagined by writers like Orwell and Huxley.

STRUCTURE OF THE BOOK

Let me say a little about the structure of this book (and my argument) before we begin. The book is divided into three parts. Part I consists of the first two chapters and essentially sets out and critically analyzes conventional understanding and theories of chilling effects. Chapter 1 examines the leading theory of chilling effects – as fear of legal harm – a legalistic account most often employed by lawyers and judges. I argue this predominant conventional account is too narrow, legalistic, and deeply flawed theoretically and empirically, and cannot explain, predict, or understand chilling effects in a wide variety of contexts. As such, it only contributes to skepticism about chilling effects, rather than dispelling them. Chapter 2 critically examines privacy-based conventional theories, which approach chilling effects as a result of privacy harms. While privacy-based theories of chilling effects improve on legal accounts, they are also too narrow and cannot explain chilling effects in a variety of contexts, including forms of privacy-related chilling effects. Moreover, courts and judges have also remained deeply skeptical of privacy-based theories. To address these limitations and fully understand the threat chilling effects pose to freedom, fundamental rights, and democracy we need a new understanding of chilling effects that moves beyond conventional accounts.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

In Part II, I elaborate this new understanding. This part consists of three chapters. Chapter 3 lays the theoretical and empirical foundation for connecting chilling effects with a broader body of social science and behavioral theory, in particular, research on social influence, like conformity and compliance. Chapter 4 elaborates a new theory of chilling effects – as conformity and compliance. I argue that chilling effects are best understood as a more powerful form of conformity and compliance – just like conformity, chilling effects reflect a behavioral tendency to self-censor and conform in the face of threats like surveillance, uncertain laws, or personal threats. The chapter also elaborates what I call the four "chilling effect" factors: observation; uncertainty; personalization or personal threats; and power and authority, which help predict and explain chilling effects. Chapter 5 demonstrates the explanatory power of this new understanding by elucidating a taxonomy of broad range of different types of chilling effects and explaining them using the theory.

Part III explores the implications of this new understanding and consists of five chapters. Chapter 6 uses this new understanding to elaborate the dangers of chilling effects both on an individual level and societal scale. Chapter 7 explains what chilling effects theory – based on the new theory advanced in this book – is for. That is, I illustrate its useful functions and applications, including demonstrating how chilling effects are weaponized against disfavored groups or to support systems of power and control; correcting flawed popular assumptions about chilling effects; and improving our understanding of privacy. Chapter 8 sets out a framework for predicting and evaluating chilling effects, including balancing them against competing chilling effects claims or competing values or public policy concerns, like speech and national security. Chapter 9 makes the case for critical changes in chilling effects law and doctrine based on the new understanding advanced in this book. Lastly, Chapter 10 predicts the "future" of chilling effects – which today looks darker and more dystopian than ever – and proposes a comprehensive law and public policy reforms and solutions to stop it.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 03:50:43, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108641784.002