# THE PRIVACY INSIDER

## How to Embrace Data Privacy and Join the Next Wave of Trusted Brands

**ARLO GILBERT**

FOUNDING CEO, osano

Osano Books

# PART 1

# HOW WE GOT HERE

CHAPTER 1

# It Started Long before the Internet

It's easy to mistake data-privacy regulations for just another compliance nuisance. Yes, they are red tape that your company hadn't needed to worry about only a few years ago. But most people don't realize that data-privacy laws have their roots in protecting human rights or that they came about *because* so many individuals' rights were exploited through the systemic misuse of personal data. That may be hard to imagine when most conversations around compliance relate to cookie consent banners and privacy policies. In many ways, we're lucky we've come so far that we, as consumers, can now exercise our privacy rights with the tap of a finger. That progress stands on the shoulders of generations of effort to get legislators to acknowledge individuals' right to privacy. And the struggle isn't over. Personal data is still accessed by others in questionable ways and used to target data subjects—whether it's to advertise to them, harass them, or otherwise exploit them.

This book starts with a quick history lesson because it's so important to realize that data privacy is about more than checking a compliance box. It's about protecting our fundamental right to privacy and the rights of our fellow humans. When you know the story behind the bureaucracy, it helps to see your privacy program for what it really is: a framework for building trust with anyone who interacts with your company.

## So How Did We Get Here?

If we want to see data privacy as more than just a complex headache, like our taxes, it helps to know how we got here. It started long before computers. The earliest privacy regulations date back to seventeenth century English common law and the Castle Doctrine, which established the legal theory that a person's home is their castle, and their castle is their safest refuge.[8] The law gave individuals the right to defend themselves and their homes against intruders, even if it meant killing an attacker in self-defense.

That may sound extreme compared to, say, protecting someone's email messages or debit card information, but the Castle Doctrine played a fundamental role in society's evolving perspectives on privacy. It was one of the first laws to grant people the right to a safe, personal space. Four hundred years later, what we consider "personal space" extends way beyond our home. And while we can't kill someone to defend everything that we consider private, the spirit of the law still resonates. We all want the right to protect what's personal to us.

US colonists brought English common law across the pond with them, and societal perspectives on privacy kept evolving with cultural, political, and technological advancements. The Quartering Act, passed in 1765, put a huge strain on citizens' right to feel safe in their homes. The law required colonists to house British soldiers. People's private

residences were spared, but colonists were forced to furnish lodging for British soldiers wherever they could: in their inns, stables, barns, alehouses, unoccupied buildings—even their outhouses.[9] The enemy was, by law, living among them. This was bad on multiple levels. In practice, colonists resented having the opposition outside their door. British soldiers lived close enough to eavesdrop on them, which was not only a nuisance and a violation of privacy but actually a criminal offense under English common law.[10] But perhaps even worse, the situation was government mandated. In the pages ahead we'll explore why a government's infringement on its people's privacy can be more dangerous than we may realize.

The Quartering Act sparked so much civil unrest among colonists that it influenced the Declaration of Independence, which counted among its grievances against King George III the "Quartering [of] large bodies of armed troops among us."[11] The Constitution's Third Amendment defies the Quartering Act, stating that, "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."[12] Colonists stood firm: they wanted the government to stay out of their private lives.

While the phrase "right to privacy" doesn't appear in the Constitution, the implications are certainly there. The Fourth Amendment defends "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," and the Fifth says, among other things, that "private property [shall not] be taken for public use, without just compensation." The Castle Doctrine was at least a century-old concept by the time the Constitution was written, but it was as relevant as ever. Colonists were doubling down on their right to a private, secure home, and they wanted just as much privacy for their personal affairs.

## The United States' Slow Crawl to Privacy Rights

It would take another one hundred years for the phrase "right to privacy" to enter the American lexicon. We can thank an 1890 article by lawyers Louis Brandeis and Samuel D. Warren for finally articulating the concept. When the article was published, society had hit a new breaking point in its perspectives on privacy. This time it wasn't war or politics that sparked the uproar—it was the media.

The printing press was one of the first technologies to influence people's opinions on privacy. Before newspapers became popular, gossip was a serious threat that could ruin reputations and economic prospects. But newspapers took the dangers of word of mouth to new heights. Now, gossip had more longevity and could cause more damage if it appeared in print. It didn't help that the newspaper industry's biggest pioneers, William Randolph Hearst and Joseph Pulitzer, were in fierce competition at the time, and they relied on drama to lure readers to their papers.[13] Yet having one's personal business in print wasn't the only problem; newspapers were also publishing photos without the subjects' consent.

Folks felt so violated by the possibility of their private business appearing in print that the outcry incited Brandeis and Warren's article in the December 15, 1890, issue of *The Harvard Law Review*. The article, called "The Right to Privacy," was a call to action, arguing that while an individual's right to privacy may be implied in common law, it should receive the explicit protection of the criminal law.[14]

Brandeis and Warren's concerns are timeless, despite the article having been published more than 130 years ago. Technology and media platforms may have changed since 1890, but much like the Castle Doctrine, the human need for privacy holds strong today. Among their concerns, they noted that "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.'" They're talking about nineteenth century newspapers exposing people's private affairs in print, but they could just as easily have been talking about Pamela Anderson and Tommy Lee's sex tape leaking to the public in 1996 or any paparazzi photographer who turns a profit by selling photos of people going about their daily lives.

The authors warned, "The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade." Truly, not much has changed over several centuries. It's remarkable how accurately their words describe the way most money is earned through the internet: your personal information is collected in exchange for access to content. In other words, the internet has opened up a trade that exists because companies can make money off of your data. We hope that companies won't overstep the bounds of decency when they process our private information, but that's just the problem. We'll see in the chapters ahead that our private information is sometimes exploited in alarming and surprising ways.

It turns out that advancements in technology only confirmed Brandeis and Warren's fears that instant photos would put people's "right to be let alone," as they described it, at great risk. They'd pointed out that before portable cameras, subjects had to sit to have their photo taken. This required their consent and gave them some control over how they were photographed. That all changed as camera technology evolved. A decade after the *Harvard Law Review* article was published, portable cameras became more accessible than ever with the release of Kodak's Brownie camera in 1900 for just one dollar (roughly thirty-five dollars in today's US currency). Suddenly, anyone could be a photographer. And the timing couldn't have been worse for those who valued their privacy.

The Brownie camera hit the market when Hearst and Pulitzer's

newspaper wars, which feasted on gossip-laden content, were in full swing. It was a troubling combination: newspapers were eager for salacious news, and now anyone could easily take candid photos of others without their consent. The Brownie camera's popularity fueled what came to be known as yellow journalism—a style of journalism that relied on sensationalized and scandalous news to draw attention. Nobody's privacy was safe as gossip could now spread and ruin reputations at new speeds.

As technology, the media, and cultural perspectives on privacy evolved into the twentieth century, Brandeis and Warren's article had a substantial influence on the privacy landscape. It filled the gaps as an authoritative source on good privacy practices at a time when related laws were lacking. Tort scholar William Prosser found that by 1960, Brandeis and Warren's article had inspired more than three hundred privacy-related cases.[15] The Supreme Court finally recognized the "right to privacy" in *Griswold v. Connecticut* (1965), stating that specific guarantees in the Bill of Rights create "zones of privacy" formed within the shadows of what is promised, even if a "right to privacy" isn't explicitly stated.[16] The right to privacy was also the basis for several Supreme Court decisions, including women's abortion rights recognized through *Roe v. Wade* in 1973 and same-sex marriage rights recognized through *Obergefell v. Hodges* in 2015.

Brandeis and Warren would be happy to see how far data-privacy regulations have come today—but they'd also likely feel that we have a long way to go. As of this writing, the United States still doesn't have a federal data-privacy regulation, despite the promise of certain proposed laws like the American Data Privacy and Protection Act (ADPPA).

I understand that the thought of *more* regulations in the pipeline may sound intimidating. It's hard enough to comply with those regulations already on your list, and for many readers, that list is getting longer every day. Companies need to comply with data-privacy

regulations based upon their users' country and state of citizenship. This means that if you hope to engage a geographically diverse audience, you must comply with regulations that are in place worldwide. The biggest in terms of global reach is the European Union's GDPR. Several others exist on national, state, and industry levels, but many of those are based on, or at least informed by, the GDPR.

The GDPR is comprehensive, strict, long, dense, and, frankly, overwhelming. The EU has historically been very protective of data privacy, and the GDPR is their most thorough regulation to date. It's easy to see it as a nuisance and simply plod through the tasks required to stay compliant, but it's worth understanding the history behind the EU's extreme caution. Its origins stem from World War II. Most people wouldn't imagine that data-privacy laws as we know them today would be linked to a war that predates the internet by decades. But once we understand the role that personal data played in violating millions of people's human rights, the connection (and the EU's concern) becomes very clear.

## Why the EU Is a Leader in Data Privacy

Germany gave us the world's first data-protection law when the Hessian Data Protection Act went into effect in 1970.[17] While it was small in the sense that it was only on the state level, it was a signal of hope for future data-privacy rights. By 1970, Germany had a decades-long history of having its people's personal data exploited. Access to personal data systems played a huge role in Nazi Germany's genocide of six million Jews during the Holocaust.[18] Government data was one piece of the puzzle, but data was exploited wherever it could be found.

In 1939, Germany's census included expanded questions about individuals' religious background. The survey asked about residents'

religious affiliation, as prior German censuses had, but this time the survey also requested information on the religious background of each individual's grandparents. The German Statistical Office used that data to create categories of "racial Jews," and any information pertaining to a person's Jewish ancestry had to be recorded on a supplementary card.[19]

The supplementary cards weren't the government's primary source in targeting Jewish populations, although some individuals' unprotected personal data did make it into the wrong hands and aided the Nazi party's genocidal mission. In all, historians and statisticians noted three distinct data sources for the deportation lists: a monthly canvass of the Jewish population that the Gestapo (the state secret police) ordered Jewish community organizations to carry out; the Gestapo card file of Jews based on unprotected personal data from the 1939 census; and a mix of police records, Jewish community organization tax and housing records, and card files of ghetto residents maintained by community organizations.[20] Personal data was misused throughout Europe for similar purposes, including in Poland, France, the Netherlands, and Norway.[21]

Many other population groups were targeted in Europe during the Holocaust. Nazis accessed personal data in the genocide of psychiatric patients, the physically disabled, people suspected of homosexuality, and the Roma population (historically referred to as "gypsies"), among others.[22] For example, it's estimated that between 220,000 and 269,500 individuals with schizophrenia were sterilized or killed during the war.[23] The victims were targeted through information that the directors of all German psychiatric hospitals were asked to share regarding the diagnosis and capacity for useful work of each of their patients. When instructed to fill out forms containing this data, the directors were not told how the forms would be used.[24]

Unfortunately, the atrocities in Europe during World War II were not the only time personal data systems were exploited

to abuse population groups. Instances of genocide and forced migration have occurred throughout history, including the internment of Japanese Americans during that same period; the forced removal of Native Americans from their territorial lands in the United States in the nineteenth century; the forced migration of minority populations in the Soviet Union in the 1920s and 1930s; and the Rwandan genocide of 1994.[25] Researchers have found that each of these events can be linked to misused personal data.

In Europe, abuse of personal information did not end with the war. When Germany led the way with the world's first data-protection act in 1970, East Germans had endured two decades of surveillance under the Ministry for State Security, also known as the Stasi. This secret police force's activities weren't monitored or regulated, and the force only answered to the Socialist Unity Party of Germany. East Germans' privacy was regularly violated under Stasi surveillance. At any time, their phone could be bugged or their intimate, personal lives spied upon. Citizens were vulnerable to violent and arbitrary arrests if there was any suspicion by the Stasi that a person was a danger to the ruling regime.[26] While the Hessian Data Protection Act only benefited people in the West German state of Hesse, the Stasi's abuse of power in the East showed what could happen when individuals' personal information was not protected. With Hesse's example at the helm, other European countries continued to lead the way. The Swedish Data Act became the first piece of nationwide legislation designed to protect citizens' personal data in 1973, and federal data-protection laws went into effect in Germany, France, and the United Kingdom over the next decade.[27] Europe understood intimately what could happen if personal data got into the wrong hands. That experience has turned European countries into the world's leaders in defending personal data, and they continue to lead the charge today.

## It All Comes Full Circle

Even if we feel we have nothing to hide, we all still have an expectation of privacy. This may look like a teenager placing a "Private: Keep Out" sign on their bedroom door to prevent a sibling intrusion, an individual trusting that they can attend a therapy session without notes being made public, or someone feeling secure that they can bank online without their account details being shared. We all value privacy and have a right to our data being protected.

If you're ever looking for a sign of the times, data-privacy laws are a great indicator. The privacy landscape is a direct reaction to evolving technology and cultural perspectives. Today's data-privacy laws are centered around how companies can collect personal information, what kind of consent they need before they can collect it, how it should be handled once they have it, and how it can be shared. Most laws also give individuals (a.k.a. data subjects) the right to request that companies share what personal information any company may store about them.

Laws are this comprehensive today because our daily activities make it easy for others to access *so much* of our personal data. Most of that activity is on the internet, but these laws apply to anything we do—whether we're exchanging Instagram DMs, signing a print copy of a rental agreement for a new apartment, or collecting emails on a clipboard at a mall kiosk.

When you consider just how much we do online, from shopping and banking to sharing photos and researching sensitive topics, it's more critical than ever that our private information remains private. In essence, our computers and smartphones have become our castle, and without regulations in place that protect our right to privacy, others can listen to what we're doing on the other side of the wall. Our need for privacy hasn't really changed over time. It's just that our culture, technology, and behavior have, and we need privacy laws

to evolve with them. The good news is, as you'll learn in the chapters ahead, the laws *are* evolving.

## TL;DR CHEAT SHEET

- Privacy rights are human rights and date back to seventeenth century English common law and the Castle Doctrine, granting individuals the right to a safe, personal space.
- The advent of the printing press ignited civilian concerns about having personal business and images printed for public consumption without consent.
- The European Union's General Data Protection Regulation (GDPR) has become the template for many national, state, and industry-based privacy regulations.
- The EU based the GDPR in part on lessons learned from WWII, specifically Germany's exploitation of census data in persecuting and killing Jews and community and police data to target people with mental illnesses, physical disabilities, and minority sexual orientations.
- Access to personal data was also exploited globally throughout history, including the internment of Japanese Americans during WWII, the forced removal of Native Americans from their land in the nineteenth century, the forced migration of minority populations in the Soviet Union in the 1920s and 1930s, and the Rwandan genocide of 1994.
- We all have a right to privacy, whether we're a teenager putting a "Keep Out" sign on our bedroom door, a patient accessing mental health or other medical treatment, or someone banking and shopping online.
- Our digital footprints and our devices have now become our castles.