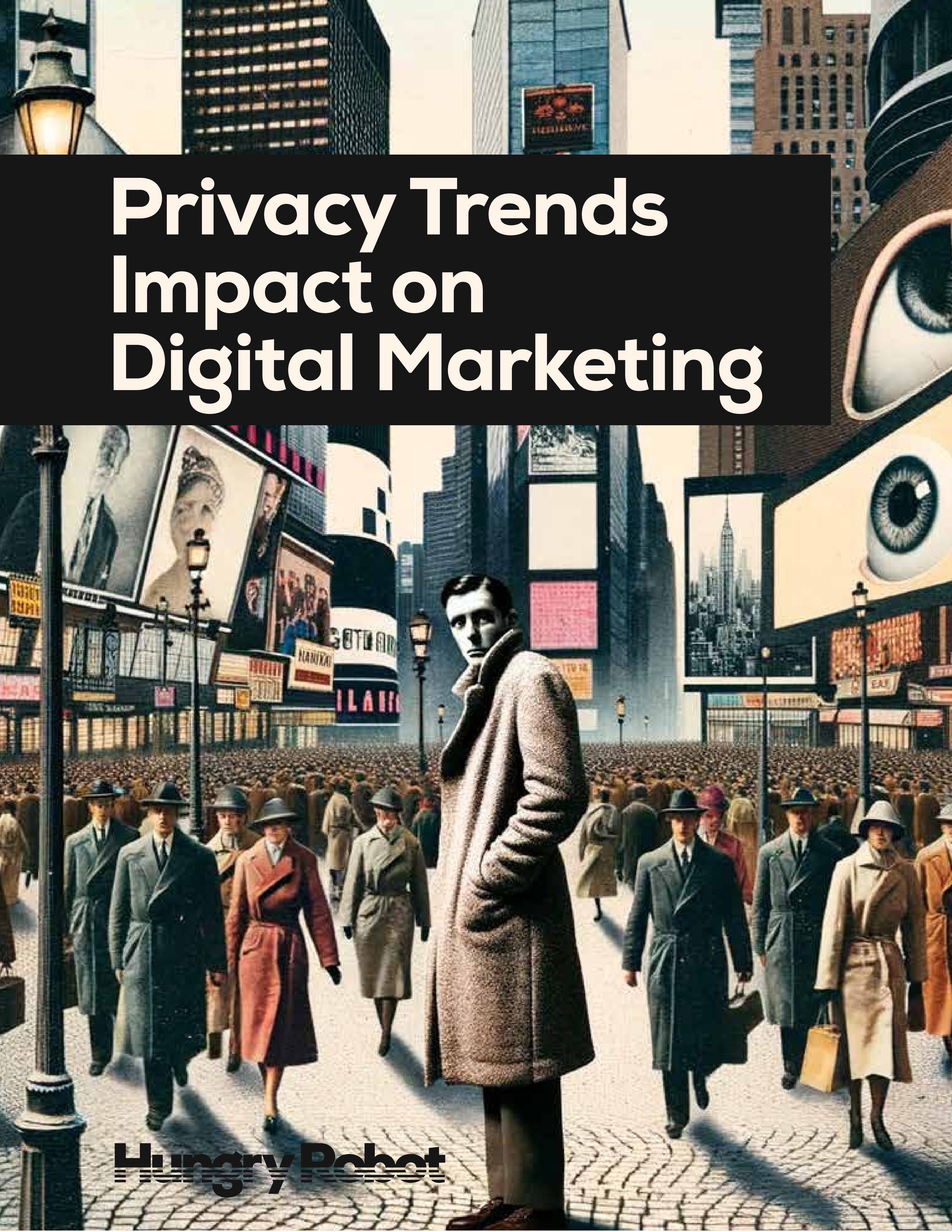
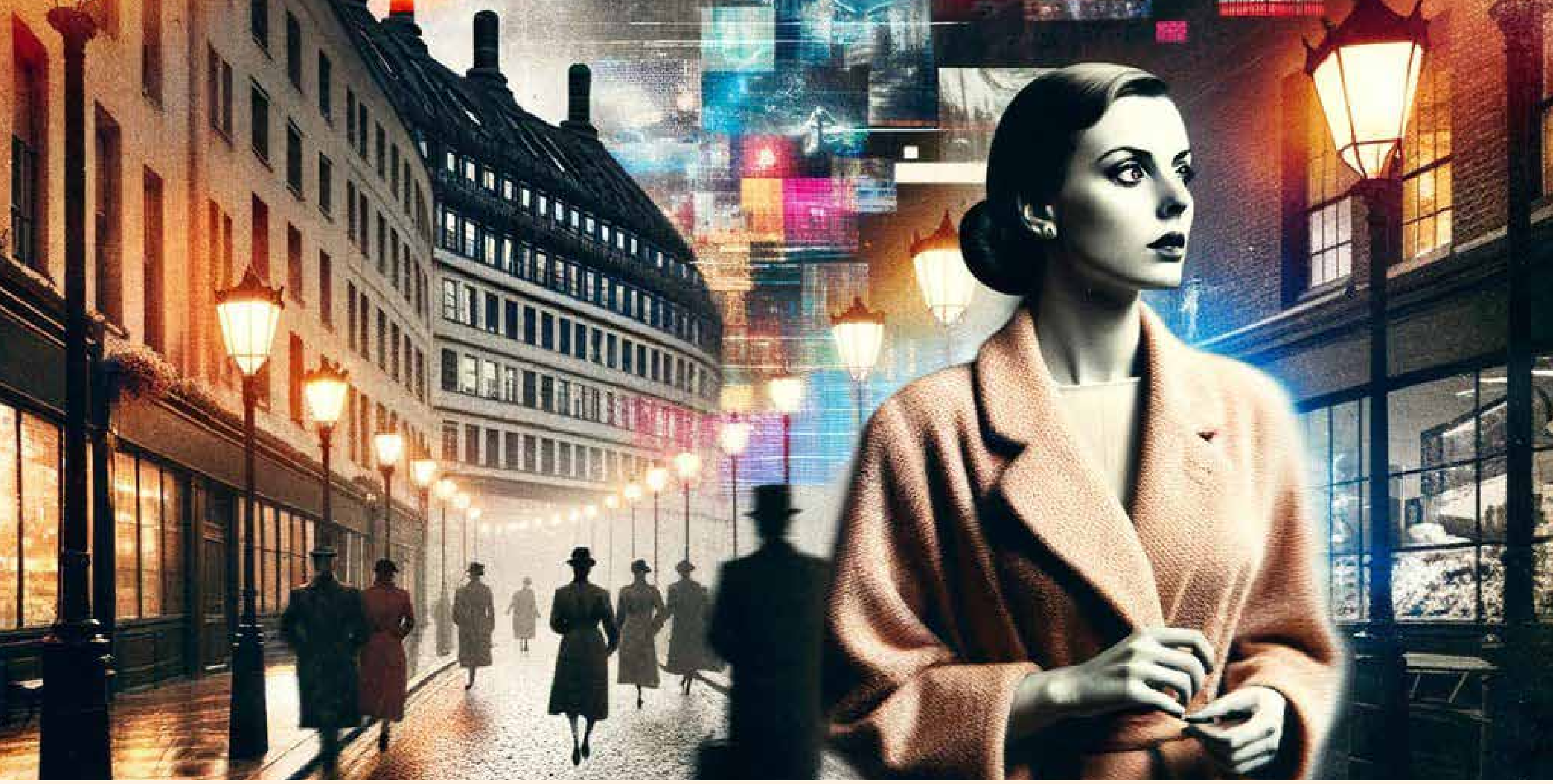
Privacy Trends Impact on Digital Marketing



Hungry Robot



Privacy Trends: The Impact on Digital Marketing

Concerns over user privacy have been rising with increasing force since the earliest days of the internet. As new legislative frameworks and technologies that safeguard user data advance, businesses that rely on measurement models from a now bygone era are scrambling, hamstrung by signal loss. The models and practices that were once reliable now introduce ambiguities that drastically compromise campaign performance because they depend on direct access to unfettered consumer data.

Recent innovations in measurement, like advanced Marketing Mix Modeling platforms, are part of a new playbook for the new Privacy Era. These privacy-resilient, holistic platforms can powerfully exceed the capabilities of online attribution methods. They incorporate tested methodologies, now expected to reshape the advertising ecosystem for years to come.

Over the past two decades, big data has been doubling in size every 3 to 4 years, and today over 98% of the world's information is stored digitally. This contributed to significant advances everywhere. For one, data science has set new standards of excellence in almost every field. From healthcare and finance to genetics and environmental studies, the ability to analyze electronic information has led to groundbreaking discoveries, more effective decision-making, and a deeper understanding of complex phenomena. This data was hyped as the "new oil," for a reason: its availability transformed commerce. Widespread access to user-level data provided even small businesses unprecedented access to consumer insights. As the proliferation of user-data ramped up alarms that started to ring every now and again as early as 1995, became louder and more constant. First in Europe then in the US, societies around the world contended with harmful externalities that gave rise to ethical questions about privacy, individual rights, and potential effects on society when every action and personal detail can be meticulously recorded and analyzed.

(For a complete timeline, scroll down to the bottom of this article.)

Where did things go wrong?

If the alpha and the omega for user privacy is the third-party cookie (privacy concerns first arrived with the invention of the cookie in 1995, and next year cookies will be phased out entirely), the technologies and businesses that were fueled by user data grew into an entire digital marketing ecosystem that overtook all of advertising. What followed were multiple privacy and security setbacks—from unauthorized collection of personal information to data breaches and widespread identity theft. These events grabbed headlines for over a decade and impacted millions. The writing was on the wall. As networked media became embedded in nearly every facet of daily life, the ongoing heated debates on ethical data usage were finally addressed in 2018 by legislation in Europe, the GDPR.

Major tech companies were also swept up in a fierce, public competition that drew a red line between privacy rights on one side and the ad platforms' reliance on user-data on the other. Apple upended the entire ad ecosystem with the release of iOS 14.5 in 2021. The update deployed App Tracking Transparency that forced third-party apps to get user consent before tracking anyone on an Apple device. Widely seen as a shot at Meta and Google, whatever Apple CEO Tim Cook's intentions, the new iOS derailed Apple's rivals but it also dovetails with his strongly held beliefs. For years prior, Cook consistently took a vocal stance on the fundamental i mportance of privacy protections as a requirement for a prosperous society. He didn't even relent FBI demands that Apple unlock a single iPhone. Undoubtedly, Apple's customers now view security and privacy as an unbreakable brand promise.

Today, for most consumers, losing control of their personal information is no longer worth the convenience and other benefits that online platforms have provided, like new connections (with friends, family, or dating). Far from it. The growing awareness about online privacy has influenced consumer behavior to take more proactive maintenance of personal information. Aside from voluntary 'Do Not Track' adoption, an increasing number of users have also made their desire for privacy clear by declining cookies whenever they are presented with the option.

This has cleared the way for Apple's iOS 17, which disables URL link IDs for both Meta and Google, further diminishing their tracking services for advertisers. Google, for its part, is phasing out third-party cookies on Chrome sometime in 2024.

Welcome to the Privacy Era.

The legislative measures passed by the U.S. and EU lay the groundwork for data privacy policy for the next century. The General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA), and the upcoming American Data Privacy Protection Act (ADPPA) enshrine privacy rights; and they mandate strict data collection and storage rules for businesses, require explicit terms for consent from users, and drastically limit user tracking. The GDPR identified three fundamental privacy rights: the right to explicit consent (data opt-in), the right to be forgotten (data erasure), and the right to data portability (switch data to competitor). These regulatory frameworks mark a significant paradigm shift: now, and for the foreseeable future online privacy will be regarded as a fundamental human right.

While privacy legislation promotes a more ethical approach to data usage, these restrictions compounded existing challenges to online measurement methods that rely on granular user-level data to track customers. The increases in signal loss dealt repeated body blows to ad platforms and advertisers, many of whom still contend with profound new responsibilities and have been slapped with fines and audits, while racing to provide new solutions to help advertisers engage with their audiences. For businesses across the board, this has forced a reevaluation of long-standing digital marketing strategies.

New Methods for Measurement

The area that is going through the most significant overhaul in recent months is measurement.

Though Multi Touch Attribution (MTA) rose in popularity as a functional, accessible foundation for measurement, now even robust MTA models are inadequate as stand-alone measurement systems. Signal loss has substantially compromised their precision and influence.

MTA works by attributing value to each touchpoint that leads to a conversion. Now, without user-level data, MTA models rely upon either rules-based or algorithmic allocations for the touchpoints that have become unobservable online. To provide marketers with more than just an approximate or theoretical reference, MTA models must be calibrated (for example, by using conversion lift studies). Without reliable data, it's increasingly difficult to evaluate the ROI of campaigns.

That uncertainty undermines planning, bidding strategies, and the validation of marketing channels.

Though attribution is still popular with the smaller, digitally native D2C marketers, this is because these businesses run small campaigns so tracking first-touch and last-click attribution suffices. Whether this can last and for how long, is up in the air. Regardless, once your advertising expands to UGC or podcasts, measuring how these marketing channels contribute to ROI is beyond reach for attribution modeling alone.

A more thorough measurement solution, like Marketing Mix Modeling is called for because it can capture the effects of real-world marketing channels, the impact of external factors, or cross-channel synergies activated across the entire "marketing mix."

Recently, MMM has reemerged as a welcome, privacy-resilient solution for measurement and guidance. This is because MMM doesn't rely on user-level attribution data. The latest marketing mix models work with aggregate information like advertising expenditure and sales figures. This aligns MMM with the demands of a privacy-first world.

At its core, MMM is a top-down statistical approach that quantifies the impact of marketing activities on target KPIs. What sets MMM apart is its ability to consider not just marketing channels, but also external factors like seasonal trends, economic shifts, and competitive behavior. This provides a holistic view of the marketing environment that enables businesses to understand not just the impact of each dollar spent, but how those expenditures interact with one another, creating cross-channel synergies that generate sales, brand awareness, or whatever the target KPIs may be.

Privacy Timeline

1994

The HTTP Cookie is invented at Netscape, and this marks the arrival of the online shopping cart.

At Netscape, Lou Montulli adopts the idea of the "magic cookie" for e-commerce client MCI. MCI did not want to be burdened with storing partial transaction states. Cookies solved the problem by enabling the users' computers that were conducting the transaction to store the data locally. Cookies were integrated into Internet Explorer in 1995, after they were patented.

Unfortunately, no one told the users that their computers were doing any of this.

1995

Amazon and eBay both launch.

The European Union takes an early position on privacy.

The EU enacts the Data Protection Initiative, which states that personal information should not be processed by online businesses at all, unless it meets conditions of transparency, legitimate purpose, and proportionality.

Internet Explorer Implements Cookies

The EU enacts the Data Protection Initiative, which states that personal information should not be processed by online businesses at all, unless it meets conditions of transparency, legitimate purpose, and proportionality.

1996 - 1997

The Financial Times starts a media outcry in the US.

By 1996, adoption of the cookie started to grow as advertisers discovered how they work. The public was largely unaware of cookies until the Financial Times published an article published that depicted cookies as a back-channel for companies to spy on consumers while they were surfing the internet. In the US, threats to online privacy became a public issue, receiving more media attention and scrutiny. This lead to two Federal Trade Commission Hearings. The FTC did not find harm, and decided to not interfere with commerce online.

This lead to two FTC Hearings in the US.

The FTC did not find harm, and decided to not interfere with commerce online.

2000

The Patriot Act

The Patriot Act lawfully broadened the surveillance powers of the NSA.

2002

The Network Advertising Initiative published a set of principles with the FTC.

NAI-compliant ad networks would provide consumers the choice to opt out of being tracked and targeted by online ads.

2003

Myspace launches.

Myspace collects user data.

User data is collected from their website and their affiliate network to select ads for each visitor through behavioral targeting.

The FTC establishes rules on Spam.

Meanwhile Spam emails attracted the ire of just about everyone, including the FTC, who makes it mandatory for commercial email senders to provide opt-outs, state their physical address, and identify ads.

2000

Mark Zuckerberg starts Facebook at Harvard.
Mozilla releases the Firefox browser.

Hacker attacks sharply rise.

These are no longer the prank hackers, but the kind that steal customer payment data. The Payment Card Industry Security Standards Council (PCI) is formed, and immediately releases the first unified security standard.

2006

Wikileaks is founded by Julian Assange.

Wikileaks starts to release material that exposes the inner workings of intelligence services, banks, politicians, and war operations around the world.

2007

Facebook launches the first newsfeed

Facebook is promptly accused of violating user privacy. Facebook then modifies the code to adjust privacy settings accordingly.

Google Acquires Doubleclick.

DoubleClick was already the largest online advertising company. The acquisition included DoubleClick's ad software, including its relationships with web publishers and advertisers.

2008

Facebook launches Facebook Connect

Through Facebook Connect, "partnered" websites can access details about the users' Facebook profile, including their full name, photos, wall posts and friend lists. Companies can legally target users with advertisements based on their behavior across several "partnered" websites.

2009

Facebook allows users to make their photos and videos private.

Permission-based email marketing arrives, requiring interested users to opt-in to email marketing. The results are higher open rates, more interested email recipients, and less spam.

2010

Instagram launches.

Mozilla competes with IE on privacy, and Google violates its policies in an effort to grow a social network.

Wikileaks releases Iraq War documents and Afghanistan War documents, provided by Chelsea Manning.

Media

The Wall Street Journal brings widespread attention to privacy concerns related to online tracking.

2011

Mozilla competes with IE on privacy, and Google violates its policies in an effort to grow a social network.

Do Not Track (DNT) is introduced by Mozilla, allowing users to express their preference not to be tracked. Microsoft follows shortly after.

The FTC sanctions Google Buzz.

The FTC finds that Google violates its own privacy policies by uploading Gmail user data into Buzz regardless if someone chose to join the social network. The settlement bans Google from future privacy misrepresentations, requires the company to implement a comprehensive privacy program, and makes regular privacy audits mandatory until 2031.

2012

Google reorganizes its products.

Google consolidates products under Google accounts, and transparently updates its privacy policy.

2012

- Facebook acquires Instagram.

All Instagram users must agree by default to allow businesses paying Instagram to display their user-names, likeness, photos (with metadata), and behav-ior as a form of advertising.

2013

- The EU ePrivacy Directive.

The EU ePrivacy Directie requires websites to inform users about the use of cookies and obtain their consent.

- Edward Snowden leaks.

Edward Snowden leaks thousands of highly classified documents from the NSA that reveal numerous global surveillance programs, run by the NSA and the Five Eyes intelligence alliance.

2014

- Apple's iCloud is hacked.

Leaked photos allegedly affected celebrities from around the world. Two years later, the leaks were found by Apple to be the result of phishing attacks. In the meantime it caused a massive uproar.

- Sony Pictures Hack

Led to the release of confidential data, destabilizing the company and affecting U.S.-North Korea rela-tions.

2015 WannaCry Ransomware Attack

- Experian is hacked.

15 million people who applied for Experian credit checks have their personal information exposed including their names, addresses, social security, driver's license and passport numbers.

2016

- Private communications take center stage during the US presidential election.

Wikileaks further inflames the Hilary Clinton email controversy, along with multiple other leaks including the DNC and Podesta emails.

2017

Apple introduces Intelligent Tracking Prevention (ITP).	Safari 11 significantly limits cross-site tracking by reducing the lifespan of first-party cookies and blocking third-party cookies.
WannaCry Ransomware Attack	Affected institutions globally, including the UK's NHS, causing widespread disruption.
Equifax breach	Exposed the data of 143 million Americans

The Era of Data Privacy Begins

2018

General Data Protection Regulation	The EU passes the General Data Protection Regulation (GDPR). The GDPR restricts how any business that comes into contact with an EU citizen can collect, analyze and store their personal data.
California Consumer Privacy Act	California Consumer Privacy Act (CCPA) is introduced. California follows the EU for California citizens by creating the CCPA.
Facebook / Cambridge Analytica and Privacy Scandals	Facebook faces at least 21 privacy scandals. When the Cambridge Analytica controversy breaks, Facebook loses $37B in market capitalization.
Google enforces HTTPS	HTTPS is enforced by Google. Websites that do not have an SSL certificate will be deprecated in Search.

2019

Apple introduces ITP 2	ITP 2 prevents first-party workarounds by resticting local storage along with third-party cookies.
Google limits third-party cookies.	Google provides an opt-out option for ad tracking cookies.
Mozilla activates Enhanced Tracking Prevention.	Firefox provides by default privacy from the third-party tracking software, through its Enhanced Tracking Protection (ETP) feature that blocks third-party cookies, along with malware protections.

2020

The CCPA goes into effect.

Google Chrome announces the Privacy Sandbox initiative, an effort to develop privacy-preserving alternatives to third-party cookies. Google replaces cookies with five APIs to retrieve data on attribution and conversions. This essentially walls off a third party's access to private information, but they still receive actionable insights.

Google introduces consent mode.

2021

Apple rolls out iOS 14.5.

The privacy update sends shockwaves through the $300B advertising industry with App Tracking Trans-parency (ATT) framework, and ends the default sharing of the IDFA. The switch to SKAd Network means limited, delayed, and less granular data. This presents new challenges to targeting and re-target-ing, advertising revenue, and install attribution.

Google Chrome to Deprecate Cookies

Google delays its plan to phase out third-party cook-ies in Chrome, partially as a result of regulatory investigations. Google extends the timeline for its implementation to 2024.

Additional States Pass Laws

Virginia passes the Virginia Consumer Data Protection Act (VCDPA) Colorado passes the Colorado Privacy Act Nevada amends privacy notice statutes, providing residents with a broader right to opt out

Amazon is fined by EU

Amazon is fined for violating the GDPR.

2022

Mozilla strips clickID Facebook, Marketo, Olytics, and HubSpot.

Meta settles Cambridge Analytica Class Action Lawsuit for $725M

The settlement is the largest ever achieved for a U.S. data privacy class action and the most that Meta has ever paid to resolve a class action lawsuit.

2023

iOS 17 strips tracking link parameters for any customized details.

Instagram is fined by Ireland.

The Irish Data Protection Commission fines Instagram for GDPR violation.

Google Rolls out Privacy Sandbox

Goolge receives guidance from UK's Competition and Markets Authority (CMA) in June and begins to enable its new privacy-focused APIs in July, with the goal of phasing out third-party cookies entirely by Q3 2024.

2023

Apple rolls out iOS 17	The update strips tracking link parameters for any customized details.
Instagram is fined by Ireland.	The Irish Data Protection Commission fines Instagram for GDPR violation.
Google Rolls out Privacy Sandbox	Google receives guidance from UK's Competition and Markets Authority (CMA) in June and begins to enable its new privacy-focused APIs in July.
California Passes "Delete Act"	The Delet Act requires data brokers to register with the California Privacy Protection Agency. By January 2026 the state will provide a website that allows consumers to have every data broker delete their personal information with a single click. Consumers will join a "do not track" list that prohibits future data tracking. By August 2026, data brokers will be required to delete all personal information at least once every 45 days and will be barred from selling or sharing new personal data.
Google sets goal of phasing out third-party cookies entirely by Q3 2024.	

Hungry Robot