CyEx | The Harris Poll

The Future of Remediation for Privacy & Pixel Cases

Data misuse, consumer impact, and a new solution to create a safer, protected future.

Table of Contents

Introduction & Background

2025 CyEx/The Harris Poll survey reveals new consumer demands for more robust, proactive protection in response to data misuse lawsuits.

Harvesting a consumer's online data has proven to be a goldmine and the buyers of this content are seemingly endless. Highly private information - like search history, medical conditions, and shopping habits - can be bought, sold, and then used to track, target, manipulate and discriminate against unassuming victims.

As businesses have adopted consumer data into nearly every aspect of their operations, headlines have often been filled with data breaches, ransomware attacks, Pixel and Privacy data misuse, and the resulting class-action and mass arbitration cases.

This paper will focus on data misuse, its subsequent consequences to consumers, and the industry's approach to remediation.

Data misuse is defined as:

The improper or unauthorized collection, processing, or sharing of personal data beyond the bounds of user consent or legal requirements. This misuse can lead to significant harm and inconvenience for victims, including financial loss, exposure of information on the dark web, emotional distress, reputational damage, and the increased risk of identity theft.

Data misuse can violate VPPA (Video Privacy Protection Act), HIPAA (Health Insurance Portability & Accountability Act), BPPA (Biometric Privacy Protection Act), and CCPA (California Consumer Privacy Act), among other data privacy laws, and lead to Privacy Class Action litigation.

While our research focuses on data misuse, the data breach category and the resultant class action actions have a long history and offers a roadmap for the data misuse category to follow. Before data misuse class action litigation became a prominent category, there was a lengthy period, still ongoing, focused on data breach class action. Early on, these lawsuits were predominantly settled by making cash payments to class members. In some instances, fines were also paid by the enterprise. Pressured to do more to mitigate the risk to consumers whose data was stolen, the industry soon migrated to a new standard for compensation to class members: credit monitoring services. While this approach was largely reactive it provided a new element of protection for impacted consumers. Recognizing that credit monitoring services alone provided diminishing value, the industry transitioned towards offering specialized identity, financial, and medical protection services to mitigate the forward risk for class members.

The data misuse category is in a similar position as data breach 20 years ago. Until recently, companies settled Pixel & Privacy lawsuits for cash payouts to class members. This did not solve the underlying issue in data misuse cases - that the affected consumers' online data, habits and information were still being sold for targeting, re-targeting and other purposes. To add insult to injury, the cash compensation was often nominal - around $30 - which is not nearly enough for a victim to compile the tools necessary to reclaim their privacy.[1] As a result, victims in data misuse cases were left with neither a solution to mitigate the loss of their own online privacy nor adequate compensation to purchase a proactive solution on their own.

Recently, a more robust model for compensation has emerged: comprehensive privacy services. Offered as part of settlements, they cover a full range of privacy concerns, including virtual private networks (VPNs), data broker opt-out, password managers, secure search, dark web watchlist capabilities and other features.

So how are these new solutions being received? Do consumers demonstrate a clear understanding of their potential? And what is holding some companies back from offering them?

Our Research

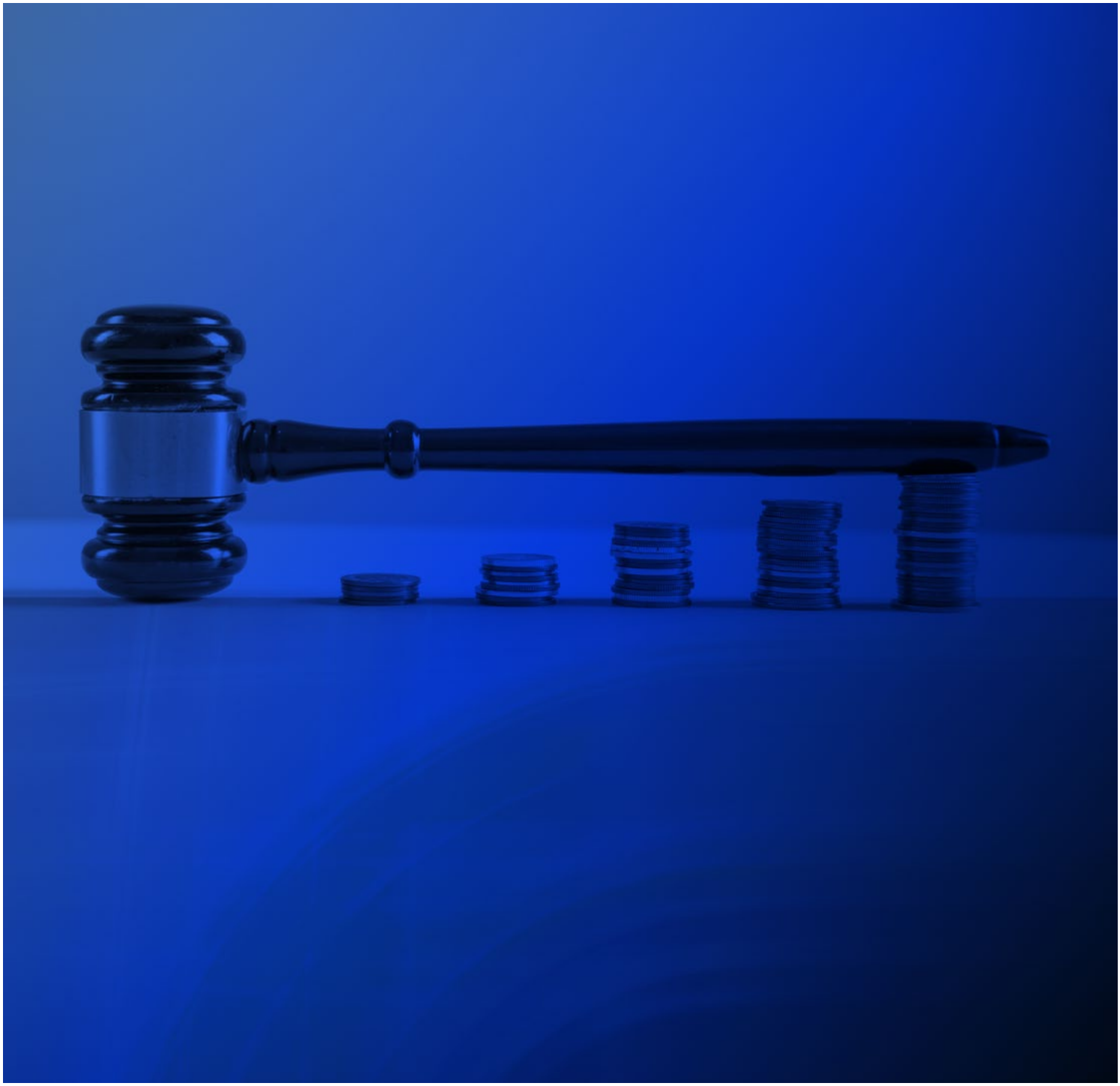
To answer these questions, CyEx and The Harris Poll conducted an online survey in June 2025 of 1,523 consumers and 207 high-level data security professionals (referred to as "data professionals" throughout this report) at medium and large businesses about their perceptions of data misuse and its remedies.

Overall, the research revealed that consumers have a growing understanding of data misuse and are seeking lasting privacy solutions rather than quick payouts. However, data professionals tend to downplay these concerns and may underestimate their significance due to the high value they place on consumer data and the multiple pathways to drive revenue through their enterprise. This appears to open up an opportunity for forward-looking companies to get ahead of consumer concerns and offer more comprehensive solutions to data misuse incidents, which could benefit businesses and consumers alike.

Differentiating Data Misuse from Data Breach:

Data misuse is different from data breach. A data breach is a security incident where sensitive, confidential, or protected information is accessed, viewed, stolen, altered, or used by an unauthorized individual or entity. On the other hand, data misuse refers to the use of information in a way that is not intended, authorized, or compliant with established policies, laws, or the original consent given by the data subject. It often involves someone who has authorized access to data but uses it for an improper purpose. Data breaches are committed by cybercriminals and outside threat actors, while data misuse is perpetrated by the enterprise that is collecting the data and selling it to 3rd parties and/or using it for their own monetization purposes.

1 (2024, June 13). $725M Facebook Settlement Payout Date Delayed by Objectors' Appeal. Kiplinger. https://www.kiplinger.com/business/facebook-settlement-how-to-claim-part-of-a-dollar725m-privacy-settlement



Problem Statement

The current standard of cash restitution for victims of data misuse fails to address the fundamental erosion of privacy caused by enterprises who collect and sell consumer data for the purposes of targeting and monetization. This leaves victims without the necessary tools or services to reclaim their digital privacy, highlighting a critical gap in effective compensation models.

Executive Summary

This report reveals that consumers have significant concerns about data misuse and a desire for better remedies when it occurs. However, it also shows that data professionals often underestimate the extent of these concerns and may be downplaying calls for more robust solutions as class action matters reach settlement.

Key findings

01 **Consumers are concerned:** An overwhelming majority of consumers express concerns about their data privacy, while only a small number say they've been unaffected by data misuse. They also report that the impact of data misuse, when it occurs, is deep and lasting, both materially and emotionally.

02 **Inadequate remedies:** Until now, class-action lawsuits have generated significant dollar value payouts, with the largest cases primarily driven by fines to the enterprise that was misusing consumer data and not always direct compensation to the class members. Consumers seem unimpressed. Whether it's the hassle of joining a class or the small payouts involved, surprisingly few people seem to want to participate in them.

03 **Comprehensive, proactive protection preferred:** Rather than retroactive compensation, consumers favor proactive protection that covers a full range of privacy concerns. Two out of three prefer to receive privacy tools to help reclaim control over their data, and almost all of them say they would use them if offered.

04 **The value of data may be clouding professional perceptions:** Surprisingly, over half of data professionals believe that users rarely experience negative impacts from data misuse. Part of the reason may be that data is so valuable they choose to ignore the downside: nearly all data professionals agree that a consumers' personal data is one of their company's most valuable assets, and most anticipate that companies will continue to misuse data even after penalties, simply treating the fines and lawsuit settlements as part of the cost of doing business.

Given that privacy concerns and data misuse are unavoidable, consumers are signaling a strong need for solutions that help them regain control over the full range of their online privacy. This desire has a larger benefit: the more people who have comprehensive protection, the less vulnerable they will be as a whole. As a result, there's a real market opportunity to introduce remediation services into all settlements thereby transforming the settlement paradigm and how it addresses instances of data misuse.

Our Findings

Our research helped to validate the problem facing consumers and businesses as it pertains to data misuse cases and provides insights that could drive recommended solutions.

Our findings are broken down into three distinct sections.

01

The Problem

Data misuse is a widespread problem and will continue due to the value it presents to businesses.

02

The Impact

Consumers experience material and emotional consequences while businesses experience impact to their reputation.

03

Improving Remediation

Consumers are unsatisfied with the current approach to remediation and desire an alternative solution in the form of privacy tools.

THE PROBLEM

Widespread experience of data misuse

Data shows near-universal fear of data misuse

How aware are consumers about data security and misuse? The short answer is: very. Whether personally affected or not, the research revealed that 9 out of 10 consumers say they are concerned about their data.

Part of the reason is that data misuse is so prevalent. Only 26% of the respondents said they had not been affected by it. As a result, trust in security is low, and consumers feel that their personal data isn't being adequately protected, which is obviously a major issue for companies that hold consumer data. While preventing misuse is the first line of defense, they clearly need to prepare for the worst and be ready to meet consumer fears and expectations where they are.

92% of consumers are concerned about their personal data.

15% are very confident companies are adequately protecting their data.

Privacy Cases on the Rise:

There has been an influx of large scale data misuse cases over the past few years. Data is increasingly being bought and sold - and the victim - the consumer. Duane Morris reported that Privacy Class Actions totaled $2.01B in 2024, up from $1.32B in 2023. By comparison, Data Breach Class Action totaled $593M during the same period. This is a massive problem that will only continue to rise.[2]

2 (2025, August 1). Class Action Review 2025. Duane Morris. https://emarketing.duanemorris.com/12/3721/uploads/duane-morris-class-action-review-2025-executive-summary.pdf

THE PROBLEM

The value of data drives businesses to downplay concerns

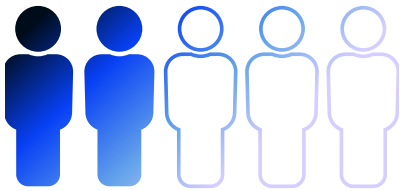
Data misuse will likely continue because customer data represents a major business opportunity

The research showed that data professionals are well aware of the issues around data misuse. For example, nearly two-thirds say that their company's users would be concerned if they knew all the ways their data was being used.

So why do companies run this risk? The simple answer is that data is just too valuable to pass up. Whether it's for marketing, product development, customer service or frankly selling customer data to the highest bidder, data is such an invaluable tool that companies seem either blind to the risks, or willing to ignore them.

97%

of data professionals believe data is one of the most valuable assets a business has today.



2 in 5

data professionals feel powerless in preventing their company from misusing personal data

THE PROBLEM

In addition, most data professionals are not as knowledgeable about laws around data privacy, like BPPA, VPPA, CCPA or GDPR, as they should be. And some don't believe it would be possible to comply with them if they wanted to. As a result, data professionals report that even after facing penalties, they expect companies to continue to misuse data.

This combination of data-reliance nearly guarantees more cases of data misuse in the future. The past few years alone have seen massive data misuse cases, including Meta ($650M)[3], and Google ($350M)[4], perpetuated by dozens of major companies, and Impacting hundreds of millions of consumers in 2024 alone. The scale and frequency of such cases means that proactive remediation is a logical and even necessary precaution, and the only way to counterbalance the effects of widespread use of a consumer's online activity.

Privacy Law	Jurisdiction	Year Enacted	Scope
HIPAA (Health Insurance Portability and Accountability Act)	United States	1996	Protects sensitive health information from being disclosed without the patient's consent or knowledge.
VPPA (Video Privacy Protection Act)	United States	1988	Prohibits the wrongful disclosure of video tape rental or sale records or similar audio-visual materials.
BPPA (Biometric Privacy Protection Act)	United States	2008	Requires companies to get informed consent before collecting, storing, or using a person's unique biological data, such as fingerprints or facial scans, and to protect that information from misuse.
CCPA (California Consumer Privacy Act)	California, United States	2018	Grants California consumers the right to know, delete and opt-out of data sales. CPRA (California Privacy Rights Act) in 2023 adds sensitive data protection.
GDPR (General Data Protection Regulation)	European Union	2018	Protects the personal data and privacy of individuals in the European Union and the European Economic Area. It also addresses the export of personal data outside these areas, requiring clear and affirmative consent for data processing.

Obligation to Protect:

Companies have specific obligations to consumers to protect and manage their data, outlined by the privacy laws above. A violation of one of these agreements, implicitly or explicitly, constitutes a path to litigation.

3 (2021, November 2). Facebook To Halt Facial Recognition After $650M Privacy Deal. Law360. https://www.law360.com/articles/1437084/facebook-to-halt-facial-recognition-after-650m-privacy-deal
4 (2024, April 3). Robbins Geller Achieves $350 Million Settlement in Securities Case Against Alphabet. Robbins Geller Rudman & Dowd LLP. https://www.rgrdlaw.com/news-item-Robbins-Geller-Achieves-350-Million-Settlement-in-Securities-Case-Against-Alphabet.html

THE PROBLEM

83% of consumers and 73% of data professionals agree that even after facing penalties, companies will continue to misuse data.

A broken social contract?

Consumers and companies have long enjoyed something data professionals call the “data social contract.” This is not a legal contract, but an implied agreement that consumers give their data to companies in return for improved products and services. However, part of this deal is the companies are also expected to protect and responsibly use that data. The survey shows that a significant feature of this contract may be broken, and that consumers are currently providing their data, and while they may be getting some value for it, companies are not holding up their end of the bargain on privacy protection.

THE IMPACT

Data misuse on consumers: material and stressful

53%

of data professionals believe users are rarely impacted by data misuse.

95%

of those who have experienced data misuse report emotional or material impacts.

This vast disconnect between data professionals and consumers highlights the root of the data misuse problem and why it persists.

Consumers experience serious consequences from data misuse

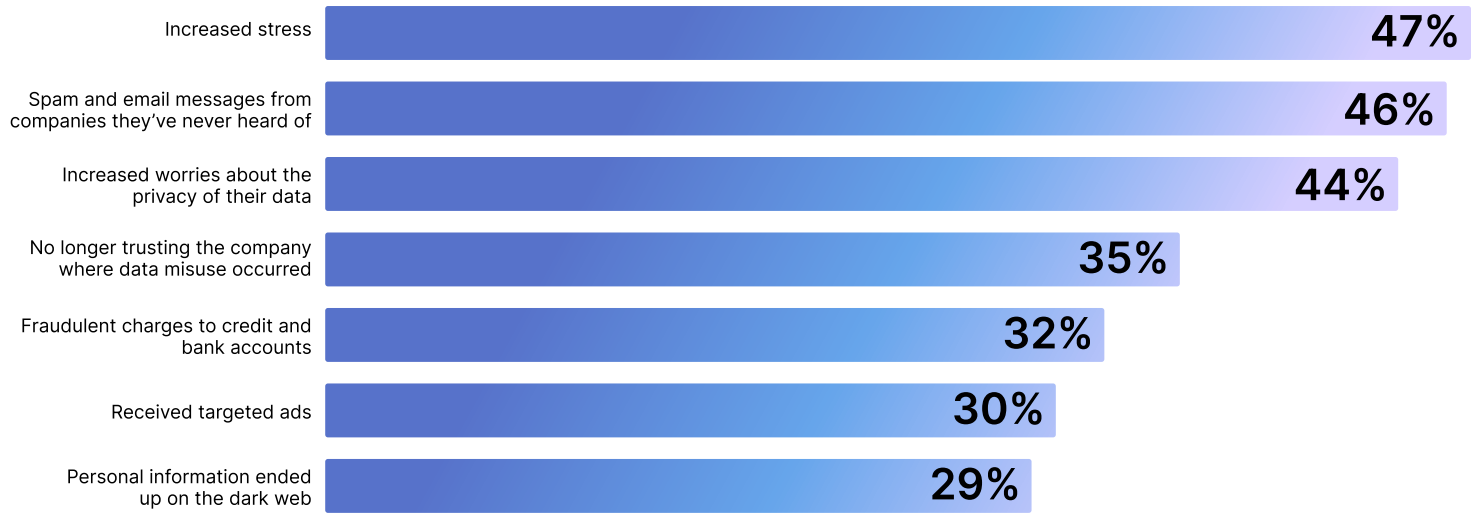
The survey also looked at the consequences of data misuse for individuals. It found a significant difference in how data professionals and consumers view this point. While nearly half (46%) of consumers report that they've been affected by data misuse, more than half of professionals believe it's a rare occurrence. The reason for this difference could well lie in how both sides define "data misuse". For an enterprise, using online activity of a consumer for tracking, targeting, resale and more is practiced behavior; for consumers that would likely be considered as pure play misuse.

However, data misuse is real, and its consequences can be severe. Nearly all (95%) of those who have experienced data misuse reported some kind of negative impact. The biggest concern was emotional, including increased stress (see chart below), while material effects were present too. Among other consequences, they reported they had:

- Received spam emails and messages from companies they had never heard of
- No longer trusted the company where the data misuse occurred
- And increasingly worried about the privacy of their data.

While 32% of those affected by data misuse saw fraudulent charges on credit cards or bank accounts, while others encountered privacy-related concerns, such as receiving targeted ads and spam emails and reputational damage.

Top impacts from data misuse

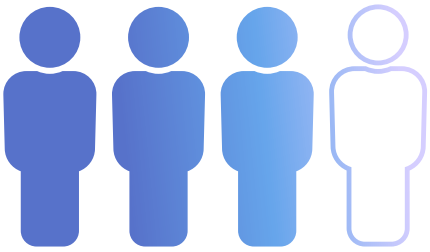


THE IMPACT

Data misuse on companies: an internal rather than external response

3 in 4

of data professionals report the most significant impacts of data misuse were internal.



74%

of consumers say that people like them do not get enough compensation from data misuse.

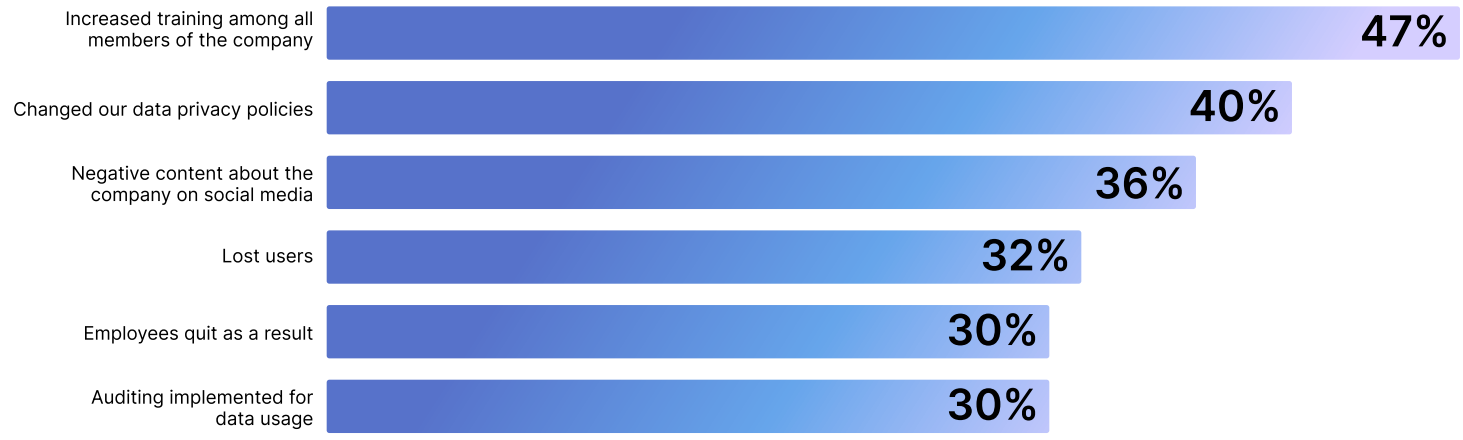
Business leaders do not understand how data misuse impacts consumers

While data professionals are aware of the risks data misuse poses to consumers, they tend to see the incidents from the perspective of their own organizations. Among data professionals whose companies have experienced data misuse in the past five years, three out of four (74%) reported that the most significant impacts were internal, not external.

The top internal impact was increased training for all members of the company (see chart below). Other major effects included changing data policies, seeing negative content about the company on social media, losing users, loss of employees, and implementation of auditing for basic data usage.

As a result, consumers are feeling under compensated, potentially also leading to feelings of being undervalued. Overwhelmingly, they disagree that “people like me usually get enough compensation from data misuse lawsuits.” This represents a substantial risk to businesses, in that consumer dissatisfaction may cause them to seek out competitors, especially if better and safer alternatives emerge.

Top internal impacts from data misuse



IMPROVING REMEDIATION

The inadequacy of current remediation

Consumers lukewarm to small cash settlements

The survey found that consumers feel broadly dissatisfied with the business response to data misuse. Nearly half (48%) say that if they received something following a data misuse incident, it would only address the impact of data misuse very little or not at all.

26%

of consumers think companies do enough to make up for data misuse.

This plays out in the legal arena as well. Although many consumers have had the option to join settlements or class-action lawsuits for data misuse, only 14% report having done so. A quarter (26%) say that the cash settlement won't be worth it. An additional 23% say that "nothing I get out of the lawsuit will make up for the data misuse."

The problem may be that class action puts part of the burden of addressing the impact of data use on the consumer. Instead, most of them agree (93%) that the company should do more to help them find an adequate solution. More than nine in ten, or 91%, wish they could do something more to reclaim control over their data privacy.

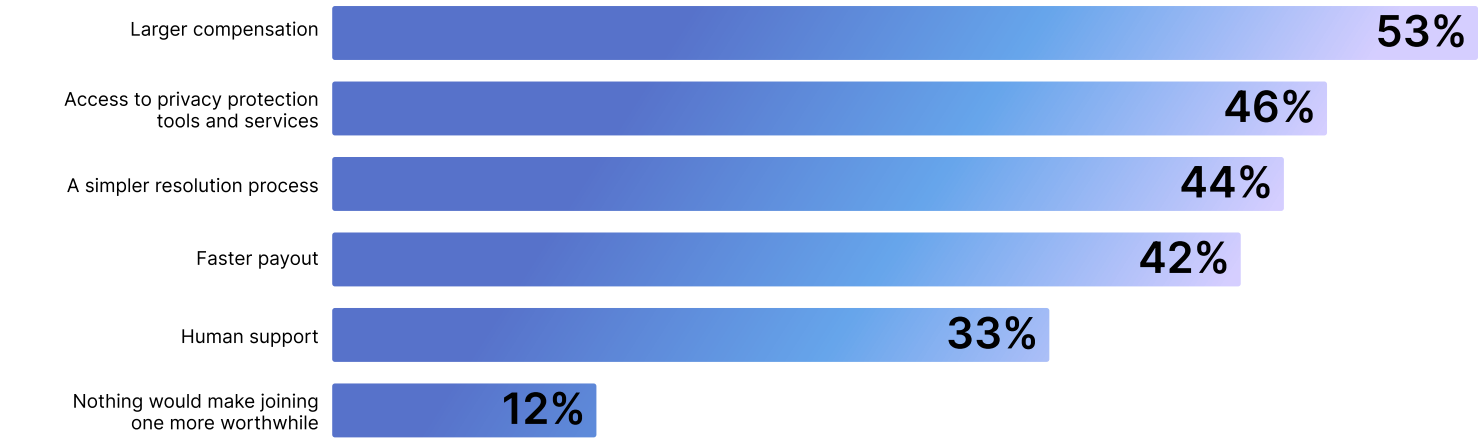
14%

of consumers have joined a class action lawsuit.

22%

of consumers who have been affected by data misuse but didn't join a class-action lawsuit said that they don't even know how to join one.

Participation in class action lawsuits may be improved with:



IMPROVING REMEDIATION

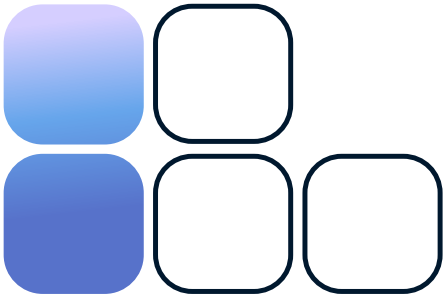
The value of proactive protection

Consumers desire tools that give them more control in the future

The research found that consumers who experience data misuse don't necessarily want a payout, especially when it is small, but rather the ability to protect themselves if something similar happens in the future. They're looking to be proactive rather than reactive; trying to fix what has happened as well as using tools to and working to create a diminished digital footprint going forward.

More than three in five (63%) would prefer to receive data privacy services and tools over a small cash settlement in the event of a data misuse incident. In addition, the overwhelming majority of consumers who are aware of tools like two-factor authentication apps and data broker opt-out apps find them valuable. And more than nine in ten agree that if they were offered privacy tools after a data misuse incident, they'd use them

The data also showed that professionals diverge substantially from consumers when it comes to compensation; most are either unaware of the preference for privacy tools or underestimate their value and impact.

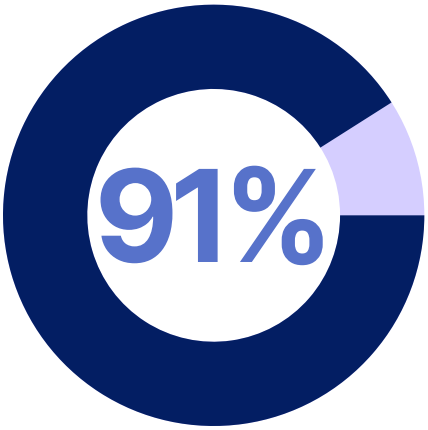


41%

of data professionals believe that users would rather have money than privacy tools.

63%

of consumers would prefer to receive data privacy services/tools over a small cash settlement.



agree that they would use privacy tools after a data misuse incident, if they were offered.

A Better Solution:

It is clear victims are looking for a solution that adequately addresses the negative impacts of data misuse incidents. The solution must help them take meaningful steps towards reclaiming their privacy and anonymity - something cash-based restitution is unable to address.

Recommendations

Data misuse is a persistent and pervasive issue in modern business. Every year, countless consumers are impacted in multiple ways, leading to alarming headlines and considerable litigation. However, the research shows that the restitution of the past, which was limited and largely financial, are no longer sufficient for consumers. Instead, addressing data misuse requires:

01 Proactive protection

Rather than seeking only monetary compensation, they are now looking for this proactive protection tailored to their unique circumstances. The industry has evolved, moving from providing cash to robust privacy solutions. The research shows that customers are increasingly open to these solutions and often prefer it.

02 New standard for remediation

Consumers are signaling an understanding and openness to a wide range of new features designed for their protection, including data broker opt-out, virtual private network, password manager, private search, digital vault, and dark web watchlist.

03 Forward-leaning companies

Joining this movement and adopting these solutions will help position insurance and legal firms for the future. All things being equal, it's better to meet consumers where they are than to try to satisfy them with compensation that does not address root causes and concerns.

04 Improving the security environment as a whole

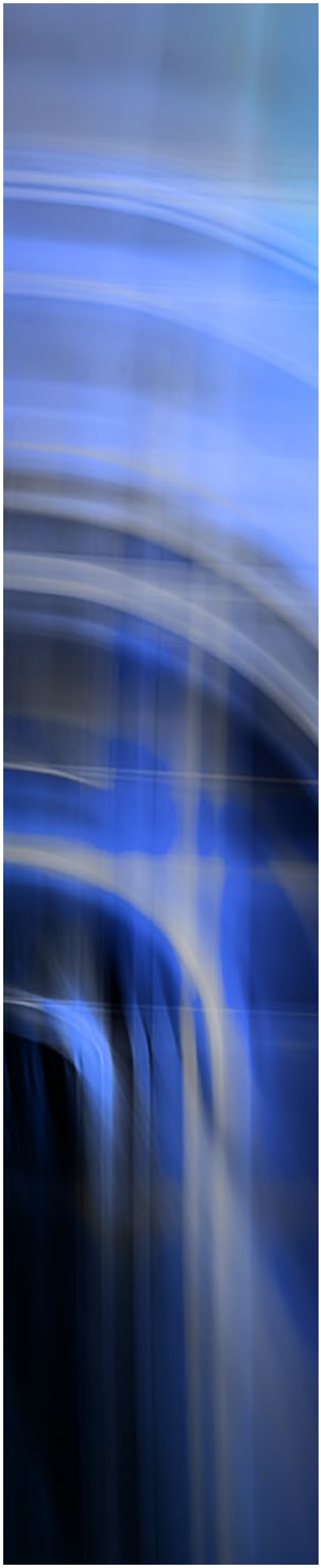
The more settlements offer proactive remedies, the more they'll help create an environment that's safer for consumers and businesses overall. In other words, giving consumers what they are demanding is not merely good public relations, but sets the foundation for fewer incidents and issues in the future.

Looking Forward

Data misuse will continue to dominate headlines, but we are also keeping an eye on future threats to consumers' privacy as Artificial Intelligence usage by enterprises becomes more mainstream. AI is poised to become the next frontier in data privacy disputes, introducing a host of complex challenges for consumers. The same highly private information that companies currently misuse—like search history and medical conditions—could be used to train artificial intelligence systems. This creates the risk of new and amplified threats, such as the creation of sophisticated user profiles and predictive models that could lead to discriminatory practices. As consumers increasingly demand more control over their information, the use of their data to develop and enhance AI technologies is likely to become a significant point of contention, perpetuating the cycle of misuse that both consumers and data professionals expect to continue.

Looking ahead, the evolution of AI will necessitate a re-evaluation of what constitutes fair data use and adequate remediation. While current settlements are shifting towards proactive privacy tools, which two out of three consumers prefer over small cash payouts, the scale and nature of AI-driven data misuse may require even more advanced solutions. Future remediation models might need to address not just the removal of data from broker lists but also the "un-training" of AI models built on improperly acquired information. This will challenge legal and technological frameworks to adapt, ensuring that consumers are protected not just from the misuse of their data today, but also from the automated decisions and potential biases of AI systems tomorrow.

CyEx is monitoring this evolving threat landscape very closely. With over 20 years of experience handling data breaches of all sizes and a history of innovating in the remediation space, CyEx is positioned to create the next generation of products to help protect consumers. Much like it launched CyEx Privacy Shield to provide comprehensive, proactive protection that goes beyond traditional credit monitoring, the company is prepared to develop new solutions to address the unique challenges posed by artificial intelligence.



Research Methodology

The research was conducted online in the U.S. by The Harris Poll on behalf of CyEx on June 4th-11th, 2025 among:

- **Consumers:** 1523 U.S. adults aged 25 years or older.
- **Data Professionals:** 207 U.S. adults aged 25 years or older who are employed full time at a business with more than 99 employees, in a director level or higher, with influence or responsibility for securing consumer data.

The consumer data are weighted where necessary by age by gender, race/ethnicity, region, education, marital status, household size, employment, household income, and political party affiliation to bring them in line with their actual proportions in the population while the data professionals' data are weighted where necessary by employee-size categories to bring them in line with their actual proportions in the population. Respondents for this survey were selected from among those who have agreed to participate in Harris Poll surveys.

The sampling precision of Harris online polls is measured by using a Bayesian credible interval. For this study, the consumer data is accurate to within ± 3.3 percentage points using a 95% confidence level. The data professionals' data is accurate to within ±8.9 percentage points using a 95% confidence level. This credible interval will be wider among subsets of the surveyed population of interest.

All sample surveys and polls, whether or not they use probability sampling, are subject to other multiple sources of error which are most often not possible to quantify or estimate, including, but not limited to coverage error, error associated with nonresponse, error associated with question wording and response options, and post-survey weighting and adjustments.

About CyEx

CyEx helps insurance companies, law firms, settlement administrators, and company owners respond quickly and efficiently to data breaches. For 20+ years, it has handled data breaches of all sizes, from small incidents to those impacting more than 95 million consumers.

CyEx Privacy Shield helps consumers reclaim control over their personal data after a breach or misuse. Launched in 2024, it's often offered as part of class action settlements – and goes far beyond traditional credit monitoring. Core features include data broker opt-out, virtual private network, password manager, private search, digital vault, and dark web watchlist. Together, these capabilities provide comprehensive, proactive protection against future data misuse for those who have already experienced it.

Learn more at cyex.com

About The Harris Poll

The Harris Poll is a global consulting and market research firm that strives to reveal the authentic values of modern society to inspire leaders to create a better tomorrow. It works with clients in three primary areas: building twenty-first-century corporate reputation, crafting brand strategy and performance tracking, and earning organic media through public relations research. One of the longest-running surveys in the U.S., The Harris Poll has tracked public opinion, motivations, and social sentiment since 1963, and is now part of Stagwell, the challenger holding company built to transform marketing.