JS|HELD

PERSPECTIVES

Data Privacy for the Future: Strategies to Limit Digital Risk and Liability

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

INTRODUCTION

Your perspectives and perceptions towards a problem drive your approach to solving that problem. Managing data privacy challenges are no different. Therefore, to address today's issues, it is a worthwhile exercise to review some past predictions, such as the a 2014 Pew Research study titled "The Future of Privacy".

In this article, we look back at predictions made, discuss these issues from today's lens, and finally closing with some strategies and solutions on how to limit the digital risk and liability emanating from data privacy issues. This article is driven by two central themes:

1. That data privacy is at the core of the digital risk and information security challenges; and
2. Whether data privacy responsibility falls to the individual, organization, or a third party.

Looking back on the 2014 Pew study, it becomes self-evident that we know what the problems are, and, perhaps, we even have good ideas of how to tackle these problems. Therefore, the issue is not necessarily "finding a solution" but rather, having the will and desire to ***implement*** a solution.

Specifically: *do we, as individuals and organizations, have the will and desire to keep our data private, or have we become so complacent and passive about data privacy, that we have, de facto, given up?*

With that in mind, we will examine the following:

1. Some 2014 predictions.
2. How these predictions held up over time.
3. Why incentives and expectations do not align.
4. Data minimization and destruction, as strategies, and why they have not taken hold.
5. How strategy is driven by incentive and not necessarily expectation.
6. What the ultimate threat vector will be.
7. Where the best solutions will likely emanate from.

FORECASTING DATA PRIVACY: DID WE KNOW IN 2014 WHAT THE FUTURE WILL HOLD?

The 2014 Pew study asked three open-ended, data privacy questions, receiving 2,511 responses from industry leaders. These macro themes emerged from the study:

- Privacy and security are foundational issues of the digital world.
- People live in an unprecedented condition of ubiquitous surveillance.
- People require little more inducement than personal convenience to disclose their personal information.
- Norms are always evolving, and privacy will certainly change in coming years.
- An arms-race dynamic is unfolding.
- Renegotiation and compromise will be a constant in the privacy-security policy space.

Additionally, the study found targeted themes we could expect by 2025, falling into two groups. The first group themes, found in the answers of those **not expecting** a widely accepted privacy infrastructure by 2025, are:

1. Living "a public life" would become the new default, where living a modern life is impossible without revealing personal information to governments and corporations.
2. There would be no way to come to an agreement on privacy and civil liberty issues on the global Internet due to varied cultures and views.
3. The situation would worsen as the Internet of Things and various devices would "tattle" on individuals, driving businesses to monetize people's data, and governments to monitor behavior.
4. The constellation of economic and security complexities would get bigger and harder to manage.

The second group themes, found in the answers of those **expecting** a trusted and reliable privacy arrangement by 2025, are:

1. Citizens and consumers would have more control thanks to new tools, giving individuals the power to negotiate with corporations and work around governments.
2. A backlash against privacy invasions would bring a new equilibrium between consumers, governments, and businesses, where savvy citizens will get better at hiding their activities.
3. Living a public life would become the new default, where some people will complain, but little objection or effort would be put into pushing back against this new reality.

HOW WELL DID THE THEMATIC PREDICTIONS HOLD UP?

At first glance, the themes appear quite on point, save for themes 1 and 2 coming from those who expected a trusted and reliable privacy arrangement. If anything, citizens and consumers have not been using new tools well, particularly as pervasive and evolving monitoring continues. Nor have their negotiating powers have been strengthened either. To use a service, the consumer is effectively forced to accept a set of terms and conditions, where in some cases, it feels as though a legal degree is needed to read them.

And while chatter exists regarding privacy invasions, backlash has not transpired. If anything, citizens and consumers are in one of the weakest negotiating positions, forced to give up even greater personal information (e.g., biometric data) to gain access to "greater conveniences" or services, and even goods.

On the flip side, it is encouraging to see that individuals are ***at least aware of the issues***. This list of 101 Data Privacy Statistics, an aggregate of multiple studies, demonstrates that sentiment for some more serious data privacy protections exists. Some key findings include:

- 71% of consumers say they would stop doing business with a company if it mishandled their sensitive data.
- Nearly 68% of consumers worldwide said they are either somewhat or very concerned about their online privacy.
- 86% of the US general population say data privacy is a growing concern for them.
- Only 29% of consumers said it is easy for them to understand how well a company protects their personal data.

But there are some troubling statistics and sentiments as well, likely driven by poor implementation of protections, difficulty understanding the protections, or bad practices:

- 33% of consumers would lose trust in an organization that uses their data to offer them products or services from another organization.
- Globally, only 29% of consumers say it is easy for them to understand how well a company protects their personal data.
- 56% of Americans say they always, almost always, or often click "agree" without reading privacy policies.
- 40% of organizations have experienced an AI privacy breach.

And for those who claim, "but privacy policies!" as a suitable protection, check out this result: *"in the US it would take an average of 47 hours every month to read the privacy policies of the 20 most-visited websites."*

Privacy policies can average anywhere between 5,000 to 15,000 words, resulting in a 30 to 60-minute read, that is neither the easiest, nor the lightest, reading. In some cases, deciphering them has been described as an "incomprehensible disaster."

For perspective, if you are reading this, you are about 1,000 words into a piece with limited legalese and a series of statistics and bullet points. *Are you up to the task of truly understanding what is being done with your data? Moreover, are you beginning to see the misalignment of interests?*

WHY INCENTIVES CONFLICT WITH EXPECTATIONS

Unless you were born and raised in some remote part of the world, where even basic electrical and water systems are considered not only luxuries, but magical marvels, some part of your life has likely been digitized. Therefore, the question is not a matter of "if" your life

has been digitized, but rather, "how much" of it has. This is where the concept of "digital risk" becomes vitally important.

Over centuries and millennia, humans have been able to adapt to physical risks and develop instincts to protect ourselves. But the same cannot be said of digital risks. In a matter of decades, our digital and computational capabilities have expanded dramatically. The same cannot be said about our habits, or more specifically, our expectations. These key issues have not kept pace with the technological changes.

In other words, **the rate of change far exceeds the rate of adaptation**, creating a delta we have been unable to bridge, or even reduce. *Why is that?*

It is because incentives conflict with habits and expectations. Be mindful, this thought track is not an indictment of our habits and expectations, suggesting we should change them. Quite the contrary. Rather, this thought track is that **we have not managed the rate of change well.**

Think back to the targeted themes of those **not expecting** a widely accepted privacy infrastructure by 2025, specifically the second theme: T*here would be no way to come to an agreement on privacy and civil liberty issues on the global Internet due to varied cultures and views.*

For a moment, **assume a culture has the expectation of personal privacy**. Can that society maintain that expectation **when that same society is incentivized to collect and use as much data as possible?** Think about the conflicts this situation creates:

- *Want to leverage artificial intelligence and machine learning capabilities for specific tasks? You need to feed the models with specific and plentiful data.*
- *Want to have a personalized experience? You need to feed the models with personalized data.*
- *Want to grow business and expand into new markets? You need to analyze more data to make better informed decisions.*

See the conflicts? Data, from a growth and innovation perspective, is almost always treated as an asset, and rightly so. ***But that same data*** is also increasingly becoming a liability, from a privacy and security perspective.

The "data balance sheet" is being hit on both sides of the ledger ***by the same item***, but the entries do not necessarily offset each other. *Are we overvaluing data on the asset side? Are we undervaluing data on the liability side?* These are the types of questions that need to be asked, and they are inherently connected.

CARROTS AND STICKS: WHAT DATA PRIVACY STRATEGIES EXIST TODAY?

Unfortunately, in a situation where data is overvalued as an asset, and undervalued as a liability, there are few "carrot" approaches out there. There are some good business cases to protect and keep data private and secure (e.g., user confidence, reputation, etc., revisit the 101 statistics to see consumer sentiment on this issue). But there are virtually no incentives to pursue data **minimization** and **destruction** strategies.

Therefore, the sentiment is "*acquire the data and protect it" and not "limit or do not acquire the data at all, or destroy what we have, because holding it is too risky.*"

Complicating matters is that we live in a very real situation where we do not even know what data we have in our vaults, which is why data mapping and classification exercises are vital to any healthy privacy and security program.

This means protection current strategies are generally driven by "the stick" making then reactive in nature. Current day "sticks" are regulations and fines, which are limited, differ jurisdictionally, can be washed down, and always reactive. This means the damage (e.g., data breach) has already been done.

Fines and court orders to institute, manage, and audit information security programs can have a positive effect, but regardless, their impact is almost felt after-the-fact.

STRATEGY IS DRIVEN BY INCENTIVE, NOT BY EXPECTATION

Using the framework we have identified (e.g., "*acquire and protect" versus "limit or do not acquire and destroy*"), we can see how defensive strategies and incentives change.

- If the model is "acquire and protect" the strategy trends go to security controls.
- If the model is "limit or do not acquire and destroy" the strategy trends go to privacy controls.

In the current marketplace, there is limited incentive to treat data as a liability, making privacy downstream from security. But to meet the privacy expectations of individuals and even organizations, that model needs to flip, where security needs to be downstream from privacy.

Imagine for a moment how organizations would react if protecting intellectual property was treated as a privacy issue and not an information security issue? Would strategies change?

Moreover, this dynamic could, at least in part, explain why Americans are feeling confused about how corporations and governments are using their data, according to the 2023 Pew Study, "How Americans View Data Privacy."

Effectively, the less you must protect, the easier and more resourceful it is, because the resources that would go into "acquire and protect" strategies can instead be invested in business operations, research and development, and all investments needed to maintain a healthy organization.

But the marketplace tells you otherwise: ***it says acquire as much as you can and do whatever you can to protect it***. Inevitably, this model becomes an infinite loop of acquiring more, managing more, investing more to protect, where the only way you break out of it is by treating the data as a liability.

Paradoxically, by breaking out of the loop, you may find yourself in a situation where less is more (e.g., less data to secure and less complex systems become easier to manage), or more appropriately, your resources become better utilized (e.g., your security investments go further, freeing up capital for other innovations and efficiencies).

THE ULTIMATE THREAT VECTOR: THE INDIVIDUAL

Going back to the 2014 Pew study, what is a common theme between those **not expecting** a widely accepted privacy infrastructure and those **expecting** a trusted and reliable privacy arrangement by 2025? *Both agreed that living a public life would become a new default*.

But what about the consequences of that new default, specifically when you combine:

1. A digitized life; and
2. The "acquire and protect" strategy?

When data breaches go bad, they usually go very bad, as we have seen from the breaches over the past few years. Once the data is breached, ***the data is out in the wild***, meaning that the intended advantages and returns (e.g., leveraging Artificial Intelligence / Machine Learning capabilities for specific tasks, personalized experiences, growth and expansion, etc.) are now coming with potentially greater costs, or costs that are hidden or difficult to calculate (e.g., what is "the dollar amount" cost your customer database being breached?).

Moreover, it feels as though an inflection point is emerging, where data already in the wild is enabling even greater data theft, feeding another loop, where more data in the wild is permitting more sophisticated attacks, such as those that use AI / ML.

Therefore, it is not entirely a surprise that the 2023 Pew study found that the American "*public expects AI's role in data collection to lead to unintended consequences and public discomfort*." This is where those familiar with artificial intelligence say its use by companies will lead to people's personal information being used in ways that people will be either uncomfortable with (81%) or in a manner that was not as intended (80%).

Now, just imagine nefarious actors have access to these data sets and technologies. The consequences, particularly

at the individual level, can include and are not limited to:

- Doxing
- Fraud
- Extortion
- Tailored attacks
- Manipulation
- Impersonation

You see, under this scenario, not only is the individual at risk, but so is the organization that the individual is tied to – because it is the individual, not the technology – which becomes both the greatest victim and faces the greatest risk.

THE SOLUTION: DATA PRIVACY AND PROTECTION BEGINS WITH INDIVIDUALS

Incentive models will not change overnight. Nor will rules, regulations, and legislation be developed quickly enough in a manner that will be universally accepted across the globe. Therefore, those in the best and most immediate position to ensure data privacy and protection are the individuals who produce and manage the data.

With that said, what we can do is change attitudes, mindsets, and behavior, focusing on a few key areas:

- **Do not give up on technical controls**. We still need these security measures, but we need to maintain them and have them operate effectively. This means regular technical testing, risk reviews, and ongoing assessment of tech stack appropriateness.
- **Shift from proactive to reactive thinking**. We are getting better. But think back to the rate of change versus rate of adaptation conversation: we will always be behind the curve. Therefore, the key is to ensure the delta is as small as possible, relative to the risks posed. Going overboard is not necessarily the answer, there is a point where investment comes with diminishing returns. Be smart about your business and your risk posture.
- **Individuals: don't produce it**. As a single user, be mindful of the data you are producing and putting out into the wild. Unfortunately, we live in a world where a nefarious actor can use every keystroke or mouse click against you. Trying to protect every action is not only unsustainable, but it also comes with both human and machine error. Things go wrong. But if the data is never produced, it cannot be used against you.
- **Organizations: don't acquire it**. This requires fighting temptation. We have burned into our heads that acquiring more data is always better. Perhaps, for a time, it was. But now, that data comes with a cost that cannot always be quantified and maybe even qualified.

CONCLUSION

Finally – and again, fighting more temptation – destroy what is no longer needed. And just in case you are hesitant about destroying it, pull it off a network, lock it away somewhere, and store it underground if you must (yes, you can do that, and many do). Data classification and data mapping are both difficult exercises, but necessary ones. The saying goes "*you don't know what you don't know*" which is why fixing data privacy issues also requires knowing what you are dealing with.

In closing, as 2025 progresses, data privacy concerns will rightly continue to exist, but we also know where many trouble points are. It is therefore up to us, especially as individuals, to protect our digital footprints and manage this digital reality that now circles all aspects of our daily lives.

ACKNOWLEDGEMENTS

We would like to thank our colleague, George Platsis, for providing insight and expertise that greatly assisted this research.

George Platsis, CCISO, is a Senior Director providing Digital Investigations and Discovery services under J.S. Held's Global Investigations practice.

George Platsis has developed and delivered strategic consulting, risk management, breach readiness and response, and complex investigation projects across multiple verticals for over 20 years. He has worked with healthcare, media, financial services, defense, construction, consumer goods, and commercial electronics. George has worked with small and medium-sized businesses up to Fortune 50 enterprises, government agencies, and not-for-profit organizations, including tailored solutions and services for executives, boards, C-Suites, and VIPs. He also has extensive experience working with law firms and insurance carriers. His interdisciplinary background spans business administration, emergency management, law, cybersecurity, and national security. He is an author, educator, content creator, and a Certified Chief Information Security Officer. As part of the Digital Investigations and Discovery service line, his focus areas are resilience maturity, digital risk reduction, breach readiness, cybersecurity proactive services, security and cyber investigations, and litigation and carrier support focusing on information, data, compromise, and security-related matters.

George can be reached at george.platsis@jsheld.com or +1 321 346 6441.