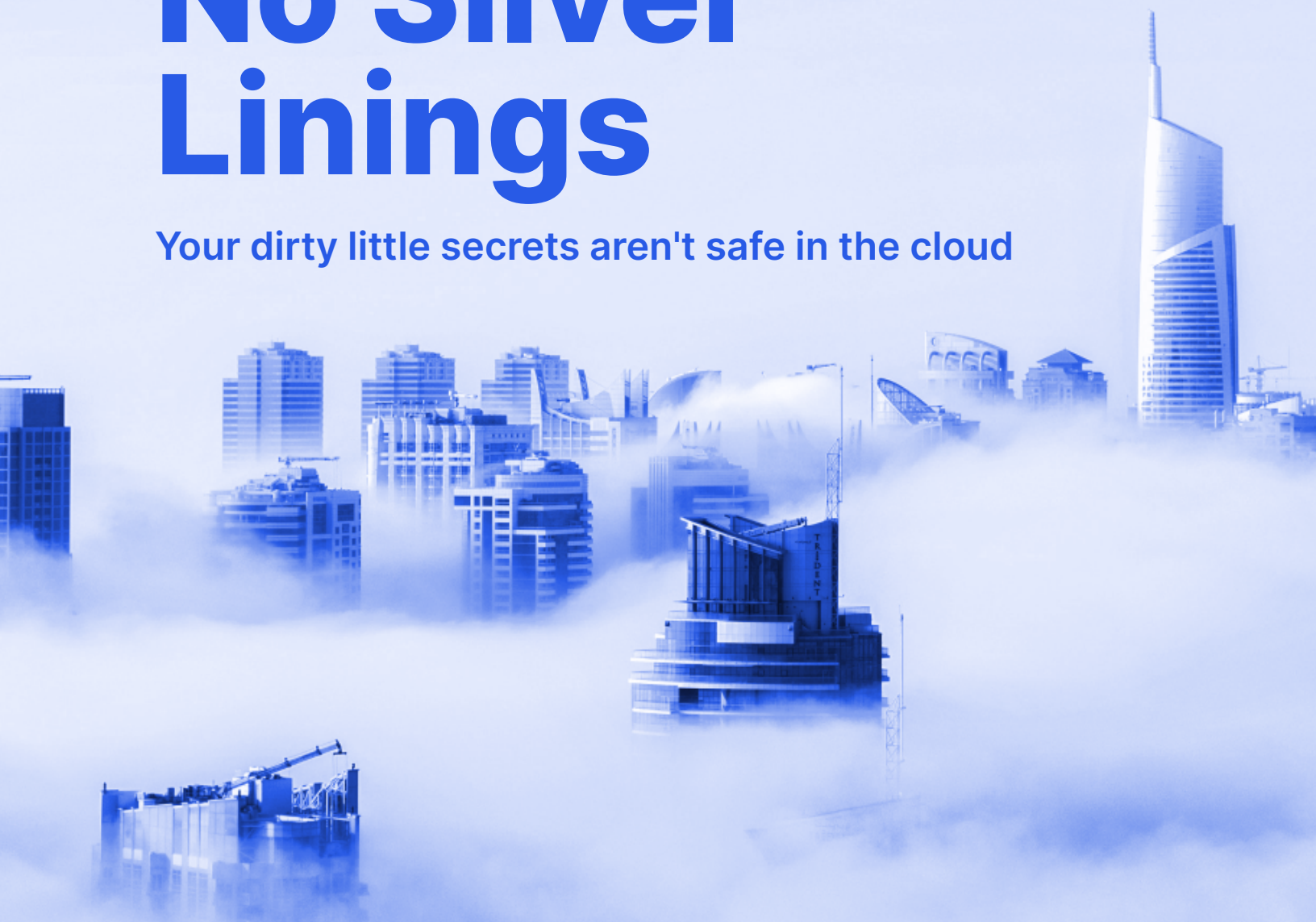
imperva

No Silver Linings

Your dirty little secrets aren't safe in the cloud



April 2022

Contents

Summary

The bottom line is this: When it comes to data sharing online, there's no putting the genie back in the bottle.

The modern mantra is that data is the new oil.

Personal information defines who we are and how we work, play, and live. It's also in high demand. The world is built on applications, systems, and networks that process and manage this data – keeping us healthy, solvent, and entertained. When done right, it enriches our lives in many ways – from deals on price comparison sites, to more accurate medical decisions.

The problem is: when an asset like personal data becomes this valuable, demand for it soars. This simple economic principle creates multiple threats for data. Whether it's stolen and sold to the highest bidder, held to ransom, or shared without consent with third parties, personal data is manipulated every second of every hour of every day. And unlike oil, data is a plentiful resource that is multiplying exponentially, making it harder to track and secure. But, do people even care? And what are the potential consequences?

To uncover these answers and understand the risk that every person on Earth faces, Imperva commissioned YouGov to conduct an in-depth, online global survey. The intent was to understand consumers' attitudes towards data, whether they feel in control of their personal data, and if they trust the organizations tasked with protecting this sensitive information.

From this global survey, three trends emerged:

Consumers are caught in a Catch-22

Most consumers (64%) feel they have no choice over sharing data online if they want to use online services. Yet, they share data so frequently they've lost track of it. A significant minority gave up caring altogether – 27% haven't bothered to change passwords that they know are compromised.

We're experiencing a data trust deficit

Almost every consumer (86%) is worried about data theft and its consequences, particularly if hackers run off with their money or identity. A majority of people (74%) say their faith in digital service providers' willingness to keep personal data secure has dropped, or at best remained unchanged, over the past five years. This is despite the introduction of stronger data privacy protections, such as the European Union's General Data Protection Regulation (GDPR) in 2018.

The cloud knows what you did last summer:

Despite this trust deficit, many consumers are still oversharing online. Two-fifths (40%) have used cloud messaging services to discuss something they'd prefer to keep private, even though 47% say doing so would ruin relationships if the conversation was leaked. More concerning, one-in-ten worry they could have their children taken away if these private discussions were exposed.

The bottom line when it comes to data sharing online: there's no putting the genie back in the bottle. Cybercriminals recognize this and won't hesitate to strike vulnerable services, extract data, and abuse stolen data. There is an urgent need for consumers to better understand the digital risks they take every day and to make more educated decisions. On the other side, there is both a moral and business objective for organizations to ensure they're doing all they can to protect privacy and rebuild consumer trust. After all, 45% of consumers say they stopped, or would stop, using a company's services if they knew it had suffered a serious data breach.

As people around the world share more of their personal lives online, and the treasure trove of digital secrets and data grows, bad actors see a ripe opportunity. With the volume of attacks and data breaches multiplying each year, companies need to bolster their defenses and prioritize the security of the data they store, manage, and access. This is now a business imperative.

A Data Catch-22

64% of consumers feel they have no choice but to share their data if they want to use online services.

It's nearly impossible to do anything online today without sharing your data. Every time you visit a website, open an application, or use a smart home device, some amount of data is exchanged. While some of it is obvious, like creating an online account with your email address, some of it is more covert. For example: the cookies that silently monitor and identify your browsing preferences for specific sites. How many even read the cookie consent pop-ups when they visit new web pages?

Around the globe, consumers feel like they're stuck in a Catch-22. A majority of people surveyed (64%) feel like they have no choice but to share their data if they want to use online services. At the same time, consumers are increasingly overwhelmed by the scale of such data collection. Many feel it has accelerated over the past two years as more services moved online during the global pandemic. That could explain why 37% are sharing more data today than they did two years ago.

37% of consumers share more data today than they did two years ago

67% of consumers have "no idea" how many organizations have their data

50% of consumers say they share data with so many companies that they can't verify each one's security track record

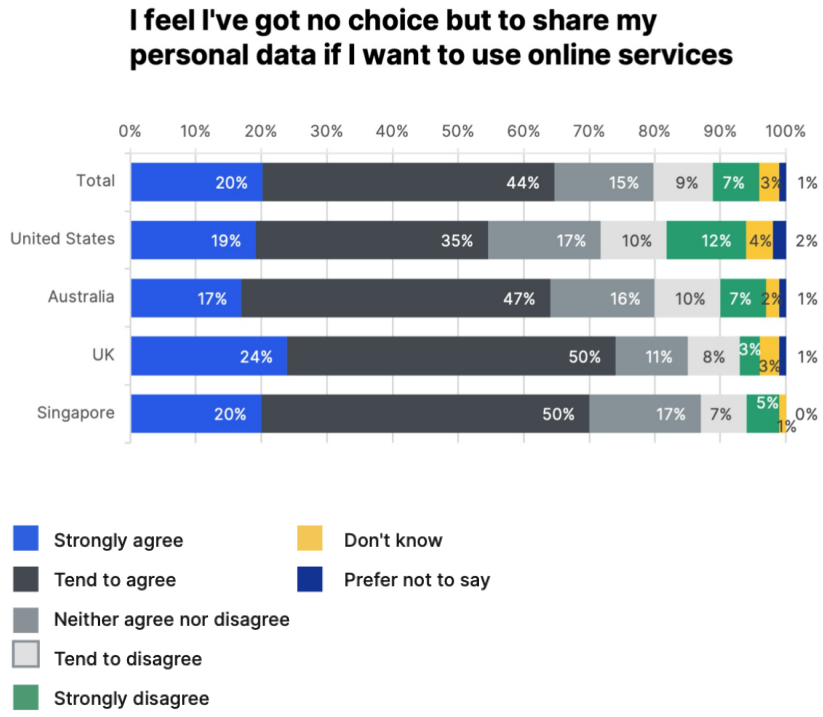
Concerningly, this makes it harder to keep track of sensitive data and how it's protected. More than two-thirds (67%) have "no idea" how many organizations they've shared data with, and 50% argue that they share data with so many companies that they can't possibly check each provider's privacy and security track record.

In short, the world is beyond the tipping point when it comes to sharing data. The risk of it being stolen, accidentally leaked, or deliberately misused is growing. In some parts of the world, data protection laws, like the GDPR, bolstered consumer rights, but it's not ubiquitous. A fractured data privacy landscape puts every consumer at risk. Even when regulations are in place, not everyone follows the rules.

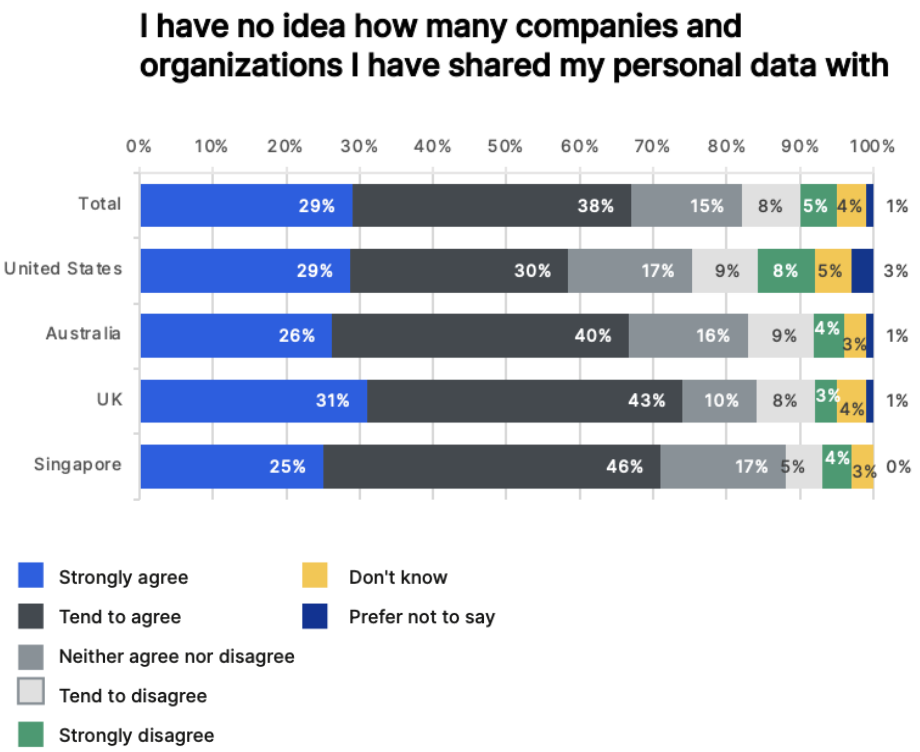
In this decade, the debate over data security and privacy will become more resounding and will have a greater influence over the future of business.

The US feels in control

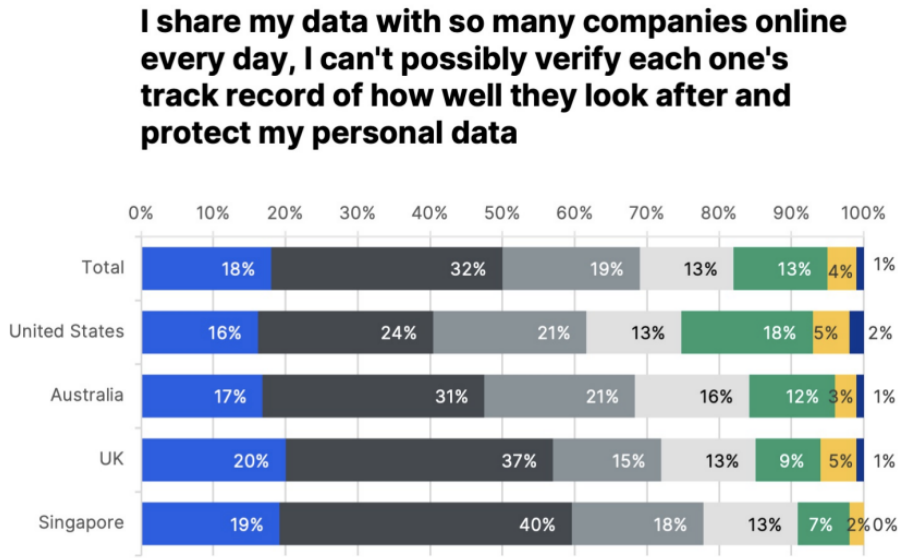
British consumers are particularly struggling and feel more overwhelmed by the scale of data sharing. Three-quarters (74%) feel they have no choice over sharing their data online, and the same proportion have no idea how many organizations they shared data with.



In the US, consumers appear to be in more control. More than half (59%) say they have no idea how many companies they shared data with, versus a global figure of 67%. Further, just 54% claim they feel compelled to share their data, versus 64% of respondents worldwide.



In Singapore, 60% feel there's no way to check the privacy track record of every company they deal with, the highest of any region.



Data Privacy: To Care or Not to Care, That is the Question

20% of consumers don't care about the amount of personal data they share online.

While most consumers feel like sharing data is required to use online services, that doesn't mean they don't care about what happens to their data. In fact, the majority appear to have concerns about privacy and data security. Sadly, this means there are still many who – whether overwhelmed by the need to share data or are simply ignorant of the risks – are giving the bad guys exactly what they want:

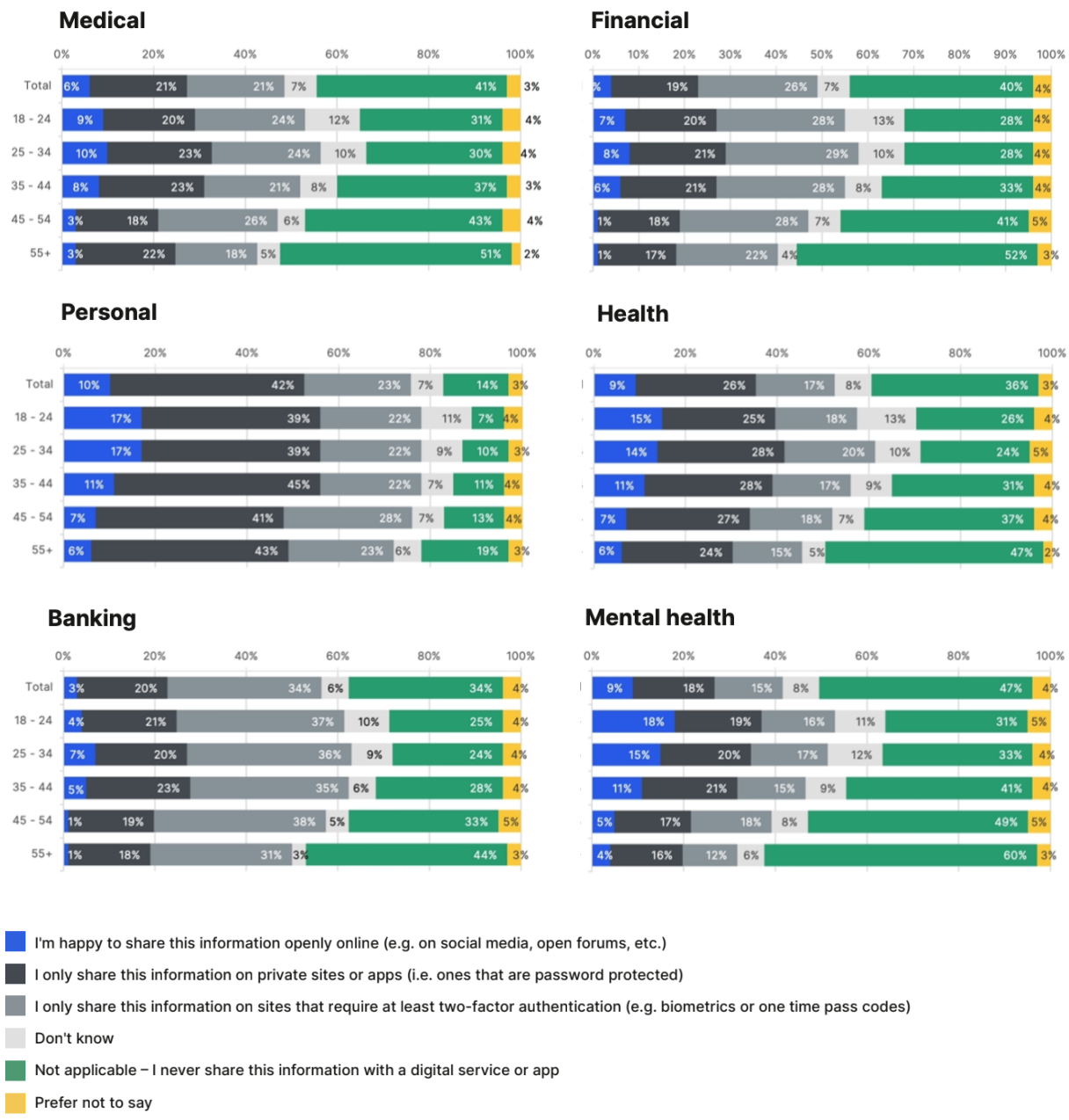
- One-fifth (20%) say they don't care how much personal information is shared online as it's already out there.
- More than a quarter (27%) say they haven't bothered to change a password after it was compromised.
- A similar proportion (26%) believe it's inevitable that their data will be compromised at some point, so they don't worry about it.

While breaches may be inevitable, the organizations that collect and manage data can make life more difficult for attackers by implementing the right security controls and tools. Consumers also play a significant part in this equation. They should embrace best practices like maintaining strong passwords, keeping device software up-to-date, and using security tools when applicable.

Are You Password Protected?

To better understand attitudes towards data sharing, we asked consumers how comfortable they are sharing certain information online, and what level of security they expect.

Attitude towards sharing types of data by age



The data suggests that passwords are merely offering the illusion of protection. Most than a quarter (27%) of people don't bother to change their passwords, even if they know they've been compromised, while others reuse passwords across multiple websites.

Meanwhile, hackers are relentlessly buying stolen credentials on the dark web and launching account takeover (ATO) attacks to impersonate and defraud innocent consumers.

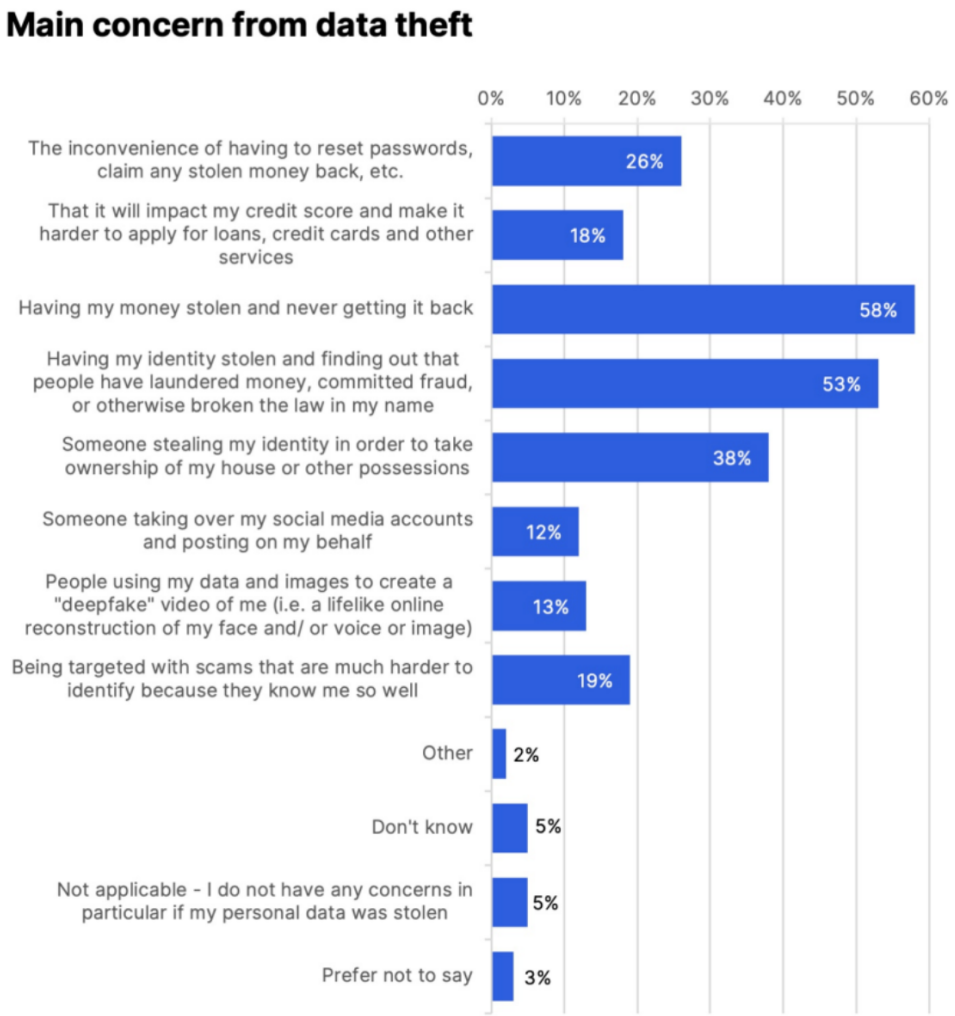
Multi-factor authentication (MFA) is a far more secure option, as it puts an obstacle in attackers' path. But at present, only a small proportion -- between 15% - 30% -- use MFA to protect highly sensitive data. A similar proportion of people trust the security of their data to sites or apps that require a password.

Not sharing data is virtually impossible, but the risks are increasing. Today, fraudsters only need a few pieces of information - often found on social media profiles - to steal an identity. For consumers, education and awareness are essential for understanding the risks involved in data sharing.

Trust is at an all-time low. More than one-third (35%) of respondents don't trust any of the industries listed to protect their data.

The Data Trust Deficit

When data breaches and security incidents are daily headlines, it can feel like a matter of when, not if, sensitive information ends up in the hands of cybercriminals. Overwhelmingly, 86% of consumers say they are worried about the consequences of data theft.



When asked to select their top three concerns, a majority (58%) of respondents cited the theft of their money and never getting it back, while Brits said this was a leading concern (70%). This stands to reason as hackers, when armed with enough personal information on their target, can open up new lines of credit, hijack online bank accounts, or use stolen card details to make fraudulent purchases.

A stolen identity, resulting in a crime carried out in their name, is the biggest concern for 53% of respondents. Nearly two-fifths (38%) are concerned about someone stealing their identity in order to take ownership of their house or possessions.

Overwhelmingly, 95% of consumers say they're worried about the consequences of data theft.

Younger people are less likely to worry about the financial impact of data theft, perhaps as they have less to lose than their older peers. However, they're more likely to be concerned about having their social media accounts hijacked, or scams involving deepfakes that impersonate them. This underscores a stark contrast between generations. Gen Z's priorities and values are focused on what harm can be done to their online reputations versus a threat targeting their property or being incriminated in fraud.

Main concern from data theft by country and age

	General	United States	Australia	UK	Singapore	18 - 24	25 - 34	35 - 44	45 - 54	55+
The inconvenience of having to reset passwords, claim any stolen money back, etc.	26%	24%	28%	27%	26%	24%	22%	25%	25%	29%
That it will impact my credit score and make it harder to apply for loans, credit cards and other services	18%	25%	14%	16%	7%	19%	19%	21%	17%	16%
Having my money stolen and never getting it back	58%	52%	55%	70%	53%	48%	48%	53%	62%	66%
Having my identity stolen and finding out that people have laundered money, committed fraud, or otherwise broken the law in my name	53%	47%	54%	58%	60%	47%	46%	50%	54%	60%
Someone stealing my identity in order to take ownership of my house or other possessions	38%	34%	38%	45%	31%	29%	30%	34%	39%	46%
Someone taking over my social media accounts and posting on my behalf	12%	11%	14%	9%	20%	15%	14%	13%	12%	10%
People using my data and images to create a "deepfake" video of me (i.e. a lifelike online reconstruction of my face and/ or voice or image)	13%	11%	16%	9%	21%	21%	16%	15%	10%	9%
Being targeted with scams that are much harder to identify because they know me so well	19%	14%	21%	19%	29%	19%	18%	19%	21%	19%
Other	2%	2%	2%	1%	1%	3%	3%	1%	2%	1%
Don't know	5%	7%	4%	5%	3%	8%	6%	6%	5%	4%
Not applicable – I do not have any concerns in particular if my personal data was stolen	5%	7%	4%	3%	6%	5%	7%	6%	5%	4%
Prefer not to say	3%	4%	4%	2%	2%	4%	5%	3%	2%	2%

Trust is at an All-Time Low

Despite the varying levels of concern that consumers have over their data privacy, protecting sensitive personal information is a critical task for the organizations that handle personal data. What this survey uncovered is that trust is at an all-time low.

When asked who they completely trust to keep their information private, consumers say they have moderate levels of trust in financial services (37%), healthcare (33%), and government organizations (29%). In contrast, consumers have virtually no trust in social media companies (7%) or retailers (5%). More than a third (35%) of respondents said they don't trust any of the industries listed.

Over the past five years, faith in digital service providers' willingness to keep data secure and protect privacy has decreased for 41% of consumers. Just 13% say their faith has increased over the same period. This shouldn't be surprising given the various data breaches and security incidents that have generated global headline news.

It's clear that organizations must do a much better job, not only of protecting data, but also being transparent about how they do this. Consumers' confidence in the process is almost as important as the process itself.

Protecting sensitive personal information should be a critical task for the organizations that handle data. Yet faith in digital service providers to keep our data secure and protect our privacy has cratered.

Trust is high in Singapore, down in the US

There's a clear difference between countries. US respondents are less trusting that organizations will keep their data safe – and only 19% trust government organizations to do so. This might be associated with the lack of regulatory control over data and privacy; the exception being the California Consumer Privacy Act (CCPA). By contrast, in Singapore, which already has strong data protection laws in place, half of consumers trust these organizations to keep their data safe.

Trust in organizations by country

	General	United States	Australia	UK	Singapore
Financial Services (e.g. Banks, insurance companies, etc.)	37%	30%	43%	40%	40%
Healthcare organizations	33%	30%	37%	35%	35%
Retailers	5%	5%	6%	5%	4%
Social media companies (e.g. Facebook, Twitter, TikTok, LinkedIn, etc.)	7%	9%	9%	3%	8%
Cloud-based messaging services (e.g. WhatsApp)	9%	6%	10%	10%	11%
Media and streaming companies (e.g. YouTube, Netflix, Xbox Game Pass, etc.)	7%	9%	9%	4%	7%
Online gaming (e.g. Xbox Live, PlayStation Plus, etc.)	4%	6%	6%	2%	4%
Government organizations	29%	19%	37%	28%	50%
None of these	35%	40%	28%	38%	27%
Don't know/ can't recall	7%	8%	6%	7%	6%
Prefer not to say	4%	5%	4%	2%	4%

The Cloud Knows What You Did Last Summer

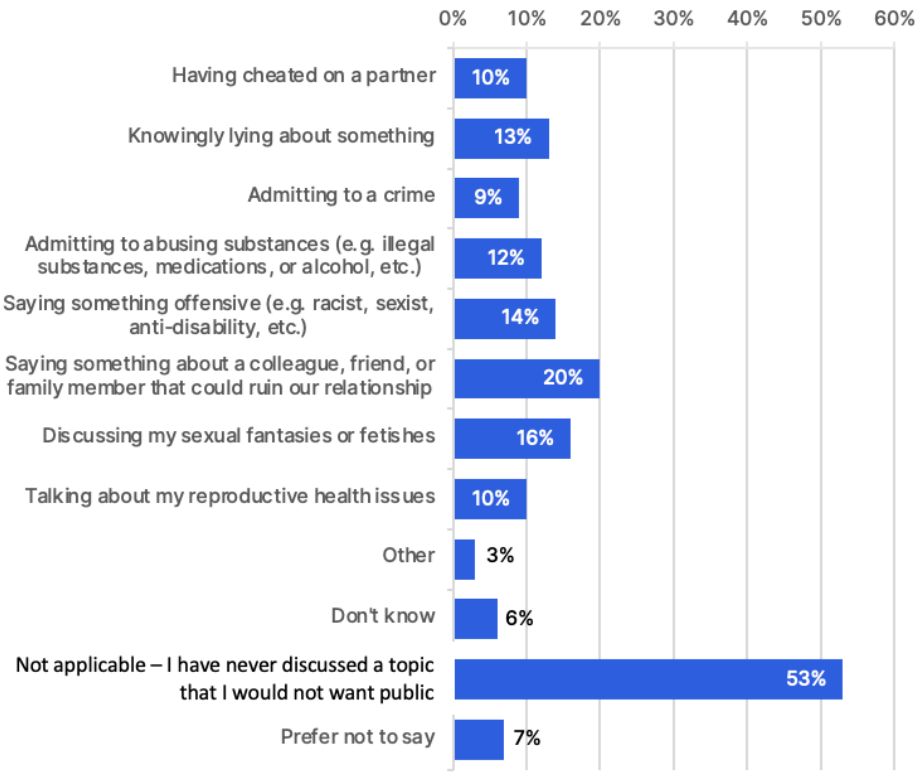
84% of people who shared their secrets with cloud messaging services say there would be **repercussions if the information they shared was leaked.**

The fight against cybercrime has never been evenly matched, but if anything, the balance has shifted in greater favor of the enemy. Cybercriminals are backed by an economy worth trillions and a vast underground world of cybercrime forums and marketplaces that exist to trade stolen data, share hacking tips, and more. Further, the paths a criminal can traverse to steal data are multiplying. They can exploit vulnerabilities in an organization's customer database, attack an insecure or misconfigured web application or API, or hijack customer accounts through compromised logins. In some recent scenarios, criminals are scraping and aggregating data and passwords using automated bots.

Organizations must protect all paths to their data, and protect them without fail. Meanwhile, attackers only have to get lucky once. Cloud-based email and messaging apps are particularly ripe targets for malicious activity given the level of sensitive data that people share (publicly or privately) on such platforms. While a lowly 9% of respondents trust these services to protect their data, it's a necessary conduit for digital life. Two-fifths (40%) of global consumers claim they've used such services to discuss something they'd prefer to keep private.

What people discuss on these platforms varies. For some, it's a conversation about a colleague, friend, or family member that could potentially ruin a relationship (20%). For others, it's a discussion about sexual fantasies or fetishes (16%). In other scenarios, people are saying something morally or socially offensive, like a racist slur or a homophobic rant (14%). In more extreme cases, people admit to talking about substance abuse (12%) or infidelity (10%) on these platforms.

Matters discussed on cloud messaging services



These are some deep and dark secrets. So, why do people continue to use such platforms if only 9% trust them? In fact, 84% of those discussing private topics are keenly aware of the risks and believe there would be repercussions if their information was leaked:

- Nearly half (47%) say it would ruin close relationships
- 39% say it would negatively impact their mental health
- 28% think they could be exposed to blackmail
- 22% say they could lose their job
- A fifth (19%) say they could lose their partner
- And 10% worry that they could even have their kids taken away.

Over the years, the world witnessed troubling cases of hacked celebrity email accounts or the release of highly personal photographs. These examples remind us that the inner sanctum of

the messaging inbox is anything but secure, and yet it's a place where many have an assumption of privacy. Yet still, people continue to share, always assuming they won't be the target.

The Brits Care for Privacy

UK consumers are the least likely (36%) to discuss private matters on cloud-based messaging services. They also admit to fewer indiscretions than their counterparts around the world; such as discussing sexual fantasies (13%), saying something abusive (10%) or admitting to substance abuse (8%), or infidelity (6%).

Young people (18+) are more likely to discuss their sexual fantasies, with almost a quarter doing so. In contrast, just 16% of respondents aged 55+ admit to discussing something they'd prefer to keep private over a cloud messaging service.

Singaporeans are highly aware of the consequences of oversharing. Half (50%) say they will never talk about a topic that they wouldn't want publicly disclosed.

Matters discussed in cloud messaging services by country and age

	General	United States	Australia	UK	Singapore	18 - 24	25 - 34	35 - 44	45 - 54	55+
Having cheated on a partner	10%	10%	14%	6%	12%	11%	13%	13%	9%	7%
Knowingly lying about something	13%	13%	16%	10%	17%	22%	21%	16%	10%	7%
Admitting to a crime	9%	10%	12%	5%	12%	12%	14%	11%	9%	6%
Admitting to abusing substances (e.g. illegal substances, medications, or alcohol, etc.)	12%	12%	16%	8%	13%	16%	18%	15%	11%	6%
Saying something offensive (e.g. racist, sexist, anti-disability, etc.)	14%	14%	17%	10%	19%	21%	20%	16%	12%	8%
Saying something about a colleague, friend, or family member that could ruin our relationship	20%	18%	21%	20%	25%	29%	31%	27%	20%	10%
Discussing my sexual fantasies or fetishes	16%	16%	17%	13%	17%	24%	23%	20%	12%	9%
Talking about my reproductive health issues	10%	10%	12%	8%	14%	13%	16%	15%	9%	5%
Other	3%	4%	3%	3%	2%	5%	5%	4%	3%	2%
Don't know	6%	7%	7%	6%	5%	9%	7%	8%	7%	4%
Not applicable - I have never discussed a topic that I would not want to be made public using a cloud messaging app	53%	52%	50%	58%	50%	31%	30%	39%	57%	75%
Prefer not to say	7%	7%	6%	6%	8%	10%	9%	8%	6%	4%

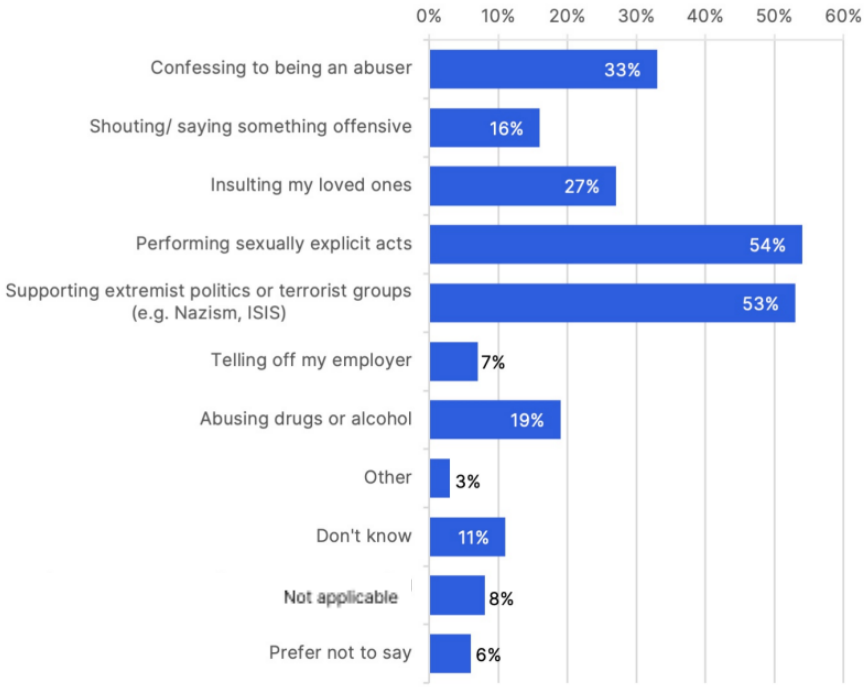
A World of Fakers

There is far more to data theft than the risk of financial loss. And the bad guys know it.

There is more to data theft than the risk of financial loss. Ransom or extortion is an increasingly popular tactic for avaricious cybercriminals. With more data available than ever before, there's plenty of opportunity. Deepfake technology represents a new front in the privacy battle. With audio and video data now readily available across every social media platform, audacious criminals can build convincing looking content to blackmail their victims. The tech itself is getting better, and the price to carry out such attacks is decreasing.

Many sites already host deepfake videos of celebrities engaging in lewd sexual acts, as the rise of deepfake porn takes hold. What worries the world about deepfakes? When asked what were the top three most upsetting acts a deepfake of them could perform, 54% of consumers said it would be a deepfake showing them performing a sexually explicit act. Similarly, 53% say the same about videos in which they show support for extremist politicians or terror groups. A third (33%) are concerned about being portrayed as an abuser. A minority (19%) worry about deepfake videos showing them abusing alcohol and drugs.

Deepest concerns around deepfakes



Deep fears over deepfakes

Women are the most likely to feel disturbed by deepfakes showing them committing sexually explicit acts (62% of females versus 45% of males), likely because revenge porn is a growing societal concern.

Respondents in the UK are the most concerned about being portrayed as an abuser: 46% would find this the most upsetting. Singaporeans are the most concerned about deepfakes: 21% identified it as one of their top three fears if their data was stolen, versus 9% in UK, 16% in Australia, and 11% in the US. They're also more likely than their global peers to be upset by images faked to show them abusing drugs and alcohol or insulting loved ones (both 27%).

Deepest concerns around deepfakes by country, age and gender

	General	United States	Australia	UK	Singapore	18 - 24	25 - 34	35 - 44	45 - 54	55+	Male	Female
Confessing to being an abuser	33%	28%	35%	46%	15%	31%	31%	33%	32%	34%	35%	31%
Shouting/saying something offensive	16%	17%	14%	10%	25%	23%	17%	17%	15%	13%	16%	15%
Insulting my loved ones	27%	23%	32%	28%	27%	24%	24%	25%	25%	30%	29%	24%
Performing sexually explicit acts	54%	48%	53%	58%	61%	52%	47%	52%	54%	58%	45%	62%
Supporting extremist politics or terrorist groups (I.e. Nazism, ISIS)	53%	48%	50%	59%	54%	53%	47%	50%	53%	57%	50%	55%
Telling off my employer	7%	8%	8%	3%	10%	7%	9%	9%	7%	4%	8%	5%
Abusing drugs or alcohol	19%	18%	22%	14%	27%	16%	18%	19%	17%	21%	17%	21%
Other	3%	4%	2%	1%	2%	2%	4%	3%	2%	2%	3%	2%
Don't know	11%	12%	10%	13%	9%	10%	10%	11%	13%	11%	12%	11%
Not applicable – I would not find any acts upsetting to be in a deepfake video of	8%	10%	7%	5%	8%	7%	9%	8%	8%	7%	9%	7%
Prefer not to say	6%	6%	6%	6%	4%	5%	6%	5%	6%	6%	5%	6%

Conclusion: It's Time for Action

We live in an always-on, digitally connected age. At the same time, the connected devices that surround us introduce security risks. The key is understanding when there's risk to be accepted, what the repercussions are, and how to minimize the chances of data falling into the wrong hands.

Yet that's only part of the story. The organizations that process and manage consumers' data have an even greater responsibility to ensure this information is protected and managed correctly. It must be secured with the highest standards. That's not just morally right, it's a sound business practice. Breaches, leaks, and other incidents have serious impacts on customer loyalty and reputation. One slip up can lead to dramatic financial repercussions.

What does good data protection look like? As an organization, you must:

- Stop thinking about application security, data security, and privacy as separate entities. Each feeds into the other, so tackle them as one.
- Understand the power of data, the various ways bad actors can use it, and the lengths they will go to do so. Realize that all customer information constitutes a potential security and privacy risk.
- Adapt your security as adversaries find new ways to compromise customer data. Apply protection to the data itself, wherever it lives and whatever form it is in.

While the cloud likely knows what most of us did last summer, it doesn't mean the rest of the world needs to have access to that information. If organizations take action now and build trust by implementing data-centric security, consumers can breathe a little easier knowing their private information is safe.

Methodology

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 6,773 adults. Fieldwork was undertaken between 22nd - 30th December 2021. The survey was carried out online. The figures have been weighted and are representative of all country adults (aged 18+).