

# From privacy vulnerability to privacy resilience

Why companies that empathize with the privacy concerns of customers and address those concerns will build a stronger business, differentiate themselves from competitors and transform workplace culture.

August 2022



Julie Brill / CPO and Corporate President for Global Privacy and Regulatory Affairs at Microsoft

We are in an era of accelerated digital transformation and rapid advances in technology. We are sharing data more than ever before and while it has simplified our day-to-day tasks, it has also increased consideration for organizations across the globe. Countries are passing regulations with comprehensive privacy requirements and within the next two years, 53% of countries will have GDPR-like regulations. With increasing complexities and changes in the regulatory landscape, organizations must ensure privacy remains central to their business.

This means that we as business leaders and security professionals must be even more focused on building and preserving trust and mindful of the timeless value of privacy. Privacy is not just a social value and a good to be achieved, but also a right, with legal ramifications.

At Microsoft, our mission is to empower every person and every organization on the planet to achieve more. With this principle in mind, we launched our first set of Microsoft Priva capabilities focusing on empowering users who deal with privacy data at their work to make smart data handling decisions.

Microsoft is proud to commission this human-centered research on data privacy and co-author this paper with privacy marketing experts. At Microsoft, we know for technology to be trusted and embraced, people need to feel assured of the safety and security it uses. The data that each of us generates is incredibly personal and it must be treated with care. It's also critically important for people and business to understand the emotional textures that play into the privacy space. Ultimately, this paper seeks to deepen our empathy with consumers' psychological experience with privacy vulnerability.



**David C. Evans, Ph.D.** Sr. Manager Customer Research, **Microsoft**. Sr. Affiliate Lecturer, Communication Leadership Program at the University of Washington. Author of *Bottlenecks: Aligning UX Design with User Psychology*, 2017. Apress Springer.

**Kelly D. Martin, Ph.D.** Professor of Marketing, Dean's Distinguished Research Fellow, **Colorado State University**. Editor of the Journal of Public Policy & Marketing. Senior Fellow of the University of Washington Sales and Marketing Strategy (SAMS) Institute and co-author of *The Intelligent Marketer's Guide to Data Privacy*, 2019. Palgrave Macmillan.

**Robert W. Palmatier, Ph.D.** Professor of Marketing & John C. Narver Chair in Business Administration, Foster School of Business, **University of Washington**. Director of the University of Washington Sales and Marketing Strategy (SAMS) Institute and co-author of *The Intelligent Marketer's Guide to Data Privacy*, 2019. Palgrave Macmillan.

**Bradley D. Olson, Ph.D.** Assistant Professor, Psychology, Co-Director Community Psychology Program, **National Louis University**. Division 48 Lead American Psychological Association.

**Peyton Hawkins**, Product Marketing Manager, **Microsoft Priva**.

## Acknowledgments

For their contributions and comments on earlier drafts, the authors wish to thank **Kacey Lemieux**, Director of Privacy Marketing at Microsoft; **Melissa MacGregor** of the Social Intelligence Practice at Microsoft; **Natalie Chisam**, University of Washington; **Jordan Tackett**, National Louis University; **Emma Beyers-Carlson, Ph.D.**, **Travis Rind**, **Danny Lam**, & **Shaina Green**, Hypothesis Group; **Mike Tapp**, **Emma Fleming**, & **Jasmin Fischer**, Share Creative.

Cite as Evans, D.C., Martin, K.D., Palmatier, R.W., Olson, B.D., & Hawkins, P. (2022). From privacy vulnerability to privacy resilience. Microsoft Corp. technical report.

**Privacy vulnerability** is the subjective feeling that consumers have when they perceive an increased risk for privacy-related harm. It begins the moment they are aware that a company collects or processes data about them, be it shared, observed, or predicted. A growing body of research shows that this perception affects commercial choices at an enormous cost to industry even if no harm occurs. Privacy vulnerability leads consumers to withhold data, abandon checkouts, switch to competitors, and spread negative word of mouth.

Replacing privacy vulnerability with a sense of **privacy resilience** is a business imperative. The research we report here shows that this opposite sentiment about personal data-processing done by organizations consists of a sense of control, security, trust, dignity and returned value. Cultivating resilience and reducing vulnerability not only reduces consumer churn, it also helps retain partners, clients, employees and shareholders. Emerging research shows that companies who authentically uphold control and transparency over personal data reduce drops in market value after actual breaches occur and after the passage of new privacy regulations.

Differentiating on privacy is thus bringing marketing and branding strategists into a conversation long dominated by legal and data experts, and it is challenging CROs and CPOs to talk about privacy externally, not just ensure it internally. Increasingly, it is not enough to point to the privacy policy, meet minimal regulatory compliance, or explain encryption technologies. **How can we talk about privacy in ways that authentically address real emotions? How can we motivate our workers to truly understand what they are protecting? We must start with human-centered research.**

This paper, open to the public, seeks to deepen our empathy with consumers' psychological experience with privacy vulnerability. We analyzed over 400,000 social media posts and fielded surveys among US and German consumers and privacy pros to understand what triggers privacy vulnerability, what emotions constitute it, and what commitments people need to hear from companies to feel resilient.

**The widespread commitment of control and transparency is a good start, but to replace privacy vulnerability with privacy resilience, companies must also address the sense of worry, helplessness, and violation that people feel when victimization is threatened, reputations are at risk, solitude is intruded upon, and autonomy and self-determination are abridged. Companies must earn trust (not demand it) by returning real value in exchange for data, giving consumers a sense of security, protecting their data ownership, and defending their due-process rights.**

These insights guide *how* to connect emotionally with consumers in external messaging. Within your company, they reveal *why* you need to invest in a privacy resilient workplace.

Microsoft is grateful to co-author this paper with marketing experts on privacy vulnerability, as well as with psychology experts on ethical approaches to social issues. We devote a special section to reigniting psychological research on privacy harm and concerns in hopes of advancing one of the great human-rights causes of our time.

# Summarizing the subjective experience of data privacy

What basic needs are served by privacy?

What threatens those needs?

What emotions are felt?

What assurances do people need to hear?

## Ownership Control

Breach  
Hack  
Identity theft  
Fraud

Vulnerable  
Victimized  
Stolen from  
Wronged  
Insecure

A sense of security  
Protection  
Compensation  
Recourse

## Spatial Control

Surveillance  
Observation  
Paparazzi

Violated  
Intruded upon  
Always on  
Self-filtered

Left alone  
Seclusion  
Peace  
Reflection

## Decisional Control

Algorithms  
Investigation  
Mandates  
EULAs

Helpless  
Manipulated  
Loss of freedom  
Held hostage

Freedom  
Empowerment  
In charge  
Choice

## Relationship Control

Oversharing  
Data selling  
Opacity  
Post-sale monetization  
Monitoring

Betrayed  
Abuse of intimacy  
Secretive  
Misled  
Taken advantage of  
Distrusted

Trust  
Intimacy  
Transparency  
Honoring agreements

## Reputational Control

Doxing  
Ransom / Kompromat  
HIPAA leak  
Right to forgetting  
Social media tagging

Judged  
Ashamed  
Labeled  
Forced conformity  
Poor impressions  
Future opportunities

Dignity  
Reputation  
Uniqueness  
In control of the future

Privacy vulnerability ⚡ triggers & 😞 emotions  
Privacy resilience 🛡️ commitments

---

*“The ability to control who knows what information about us and to limit intrusions into the solitude of our lives, privacy is intrinsic to individual dignity and our sense of personhood, to our ability to live as unique beings.*

*Privacy allows us to test our ideas and to live without undue scrutiny. It lets us choose our relationships, overcome our pasts, direct our future, and change our minds and our behavior over time.”*

# Table of contents

08 /

What is privacy  
vulnerability and why  
is it so costly?

28 /

The commitments that  
foster privacy resilience

40 /

Inspiring the study of  
privacy psychology

14 /

Situational triggers of  
privacy vulnerability  
discussed online

32 /

Privacy resilience is a  
differentiator

46 /

Endnotes

21 /

The emotional  
texture of privacy  
vulnerability

36 /

Move your company  
up the privacy  
resilience spectrum

# What is privacy vulnerability and why is it so costly?

# What is privacy vulnerability and why is it so costly?

A body of research is emerging that suggests that people's subjective feelings of privacy vulnerability around a company's data management practices can strongly affect commercial outcomes—even if the parties involved never suffer a breach.

An extensive literature review combined with consumer-level experiments and models of the actual impact of data breaches on abnormal stock returns (Martin, Borah, & Palmatier, 2017) found that most people experience feelings of privacy vulnerability just knowing that a company has access to their data. As soon as they click "submit" to transfer personal information, or become aware of the passive data-collection of profiling data or "digital exhaust" (see Morey, Forbath & Schoop, 2015), vulnerability kicks in. People have a keen sense of when their private information is being accessed, putting them at greater risk of some privacy-related harm, even if no harm ever occurs.

In this paper, we explore the emotional texture of privacy vulnerability and ways to alleviate it, but published research already suggests that it can cause people to take action such as disengaging with a company or spreading negative word of mouth. Privacy vulnerability can both impair company performance directly as well as exacerbate the negative abnormal stock returns that occur after an actual breach.

Fortunately, the reverse is also true: minimizing vulnerability through authentic promises of "transparency and control" suppresses the negative results of a breach.

**One enterprise company in the model could have reduced an estimated \$836 million loss in market value after a privacy breach to only \$16 million had it offered its consumers greater transparency and control related to the use of their personal information (Martin et al., 2017).**

Consumers continue to experience privacy vulnerability through their engagement journey (Okazaki, Eisend, Plangger, de Ruyter & Grewal, 2020). For example, during pre-purchase, consumers generate a lot of behavioral surplus from information gathering and search queries. Anticipating consumers' decisions or revealing highly specific search-informed options can not only feel "creepy" or "stalking," it can make people abandon the engagement altogether. During purchase, data requests can have a similarly chilling effect if information is sought that is beyond the reasonable scope of how a consumer might use the product or transact with the company.

Consumers may also wonder how long such information will be retained. Finally, the post-purchase phase of the journey may continue to generate data, and a firm will need to walk a fine line on the ways in which this is used. Availing that information to partner firms that can suggest complementary or accessory products might provide consumers value, but it can also appear like a further money grab from the original selling firm.

It may be tempting for companies to conclude that strong security protections adequately address privacy vulnerability. But confirming what most privacy professionals believe, security is necessary but not sufficient for privacy. Research shows that even the most robust cybersecurity stance is not enough when it comes to the level of trust that people feel when interacting with a company and deciding to share their personal information (Martin, et al., 2020).



---

*“Consumers continue to experience privacy vulnerability through their engagement journey.”*

---

Okazaki, Eisend, Plangger, de Ruyter & Grewal, 2020



## Privacy vulnerability and regulatory changes

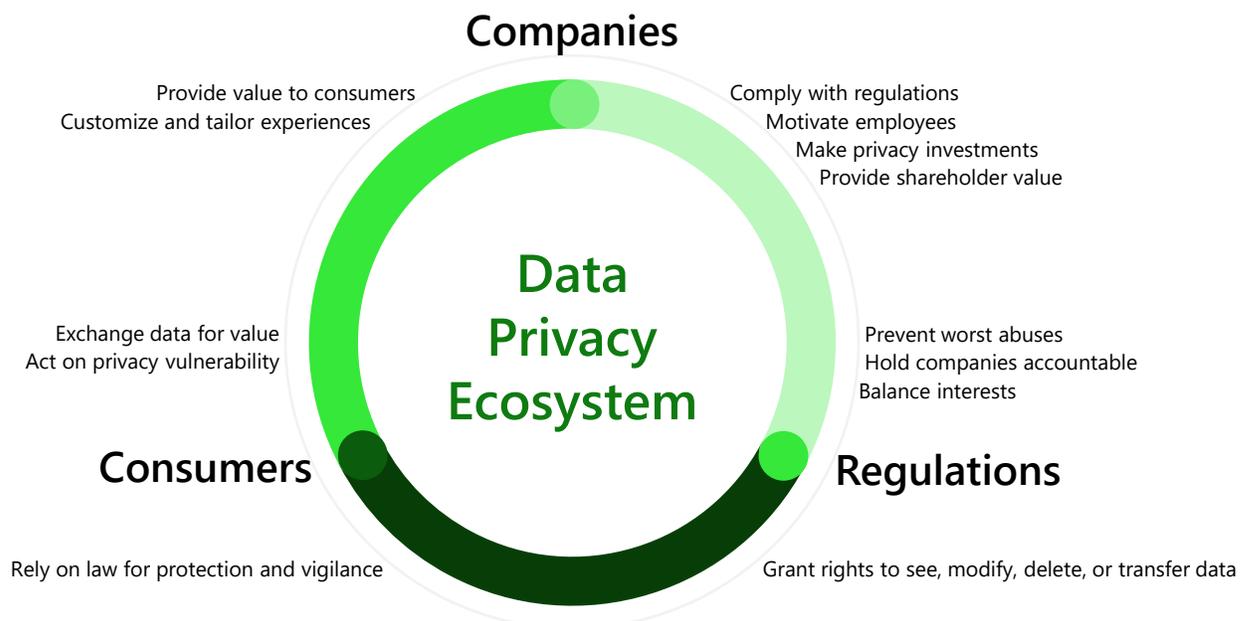
Research also shows that the sense of privacy vulnerability differs depending on the regulatory environment and local cultural norms (Martin et al., 2020). A multi-country study on privacy perceptions revealed that people in countries with strong data-privacy protections and widespread views that personal privacy is a human right (e.g., Germany), have a much lower threshold for feeling privacy vulnerability and a much higher threshold for trust. Folks in countries with strong privacy protections are unwilling to share certain dimensions of their personal information, even for significant compensation.

The picture is more complex in the United States. Compared to Europeans, Americans have been conditioned to believe their information has less value. In some ways, they show a willingness to believe that their data can belong to a company for very little in

return. And yet, in the absence of a national-level framework like the GDPR in Europe, Americans reflect the perception that they have less in the way of regulatory protections and legal recourse. This can also increase their subjective sense of vulnerability.

In any case, new research shows that the interplay of privacy regulations and the sense of vulnerability is also impacting investor decisions. A modeling exercise reported in a working paper at the University of Washington (Chisam, Germann, Palmatier, 2022) shows not surprisingly that the passage of new privacy regulations can trigger investor skittishness. Investors worry that the regulations can increase legal costs and create risks to brand reputation and compliance or put a damper on competitive innovations involving data use. This bump in the road can be even worse for smaller companies.

### EXHIBIT 1. DATA PRIVACY ECOSYSTEM



But once again, privacy resilient workplaces reduce the sense of vulnerability in investors just like in consumers. How do they become resilient? The modeling showed first that they store their data externally in the cloud and leverage the cloud providers' privacy protections. One privacy pro we interviewed said that when "a new privacy law comes to bear, it would be more challenging for you to meet those standards because you don't have that single resource like a cloud vendor has," adding that quite often, cloud providers' "level of security goes beyond what any of these regulatory standards require." With this backing, privacy resilient companies make strong public commitments to uphold the transparency in their data usage and the control that consumers have.

The payoff can be quite significant. In the models, the range in abnormal stock returns between the most and least resilient companies after a new privacy regulation is passed was 3.7%.

That equates to \$736 million in market value. As one privacy pro summarized the companies that best adapt to new privacy protections, "If their reputation is well deserved, they will be ahead of the curve in compliance and already have adopted a lot of those practices."

Companies that become convinced that reducing privacy vulnerability and projecting privacy resilience is a differentiator lean into cloud investments and privacy messaging. But claiming the privacy high ground still requires resonant, empathic messaging that must also overcome the headwinds of bringing up a topic most would prefer to ignore.

That's why we next looked deeper at the psychology of privacy vulnerability. What triggers it, what is its emotional texture, and what commitments mitigate it? Understanding this is essential to alleviating the sense of vulnerability.

**"You never know what's going to happen to your data once you've entered it. They may sell your data."**

DE Consumer

**"I've actively tried to prevent skimming because swiping your credit card means your credit card's going to this nefarious person."**

US Consumer

# Situational triggers of privacy vulnerability discussed online

# Situational triggers of privacy vulnerability discussed online

Our first original study examined 412,511 conversations in social media from February 2021 through February 2022 to learn what people say online when they feel a sense of privacy vulnerability. (See the appendix for full methodological explanations of our research.)

We uncovered seven topics which revealed that when people take to social media to discuss privacy vulnerability, they focus on the situational antecedents (triggers) more so than their emotional reactions (which we thus devoted our surveys to exploring). (See Exhibit 2) These topics represent consumer thinking most directly, but don't forget that every privacy pro and investor is also a consumer.

Undoubtedly, privacy vulnerability leads to negative word of mouth which spreads at scale online. If a company triggers privacy vulnerability, folks are likely to post about it. Their motivation tends to be to hold companies accountable and to raise their social capital among their peers by warning others to avoid the bad experiences they had (Evans, 2017). Companies and their brands want to stay far away from this "naming and shaming." When consumers are not influencing others about which companies value privacy, they are often sharing best practices in privacy and security protection (see the "cybersecurity tips" topic in Exhibit 2).

## EXHIBIT 2. TOP DATA VULNERABILITY TOPICS EXPRESSED IN SOCIAL MEDIA (t-SNE MAP 2021)

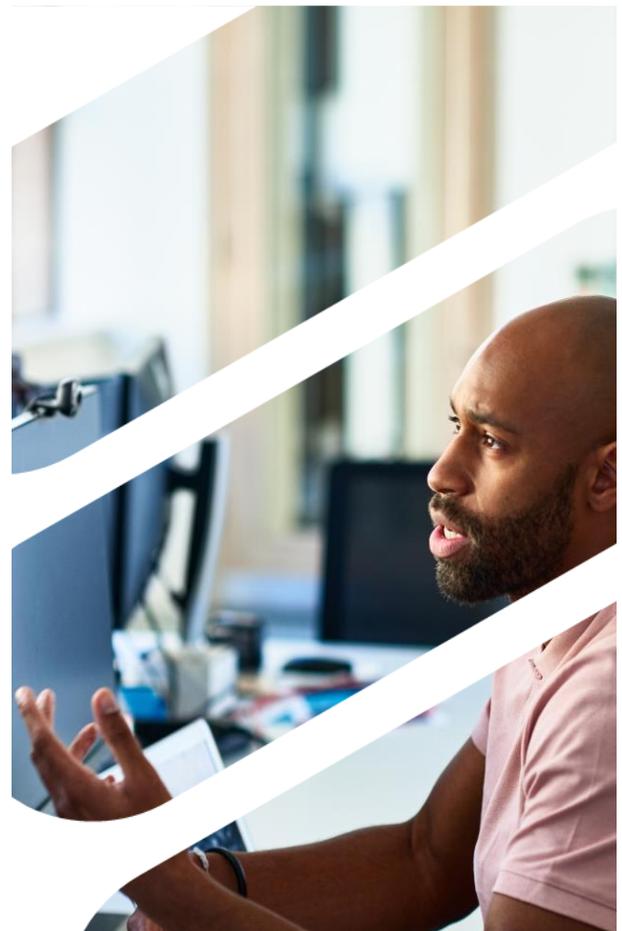
Visual representation displayed, for the actual map [click here](#)



The next takeaway is that a wide variety of industry sectors arouse privacy vulnerability. Companies in healthcare, consumer technology, communications, entertainment, social media, government, law enforcement, and retail (particularly as it relates to parenting and family products) can trigger privacy vulnerability. Privacy vulnerability can also be triggered by media coverage of these industries. In a time when it is said that “data is the new gold” and many companies are incubating innovations with consumer data, it appears that few if any get pass from the privacy vulnerability pressures affecting their business success.

The final takeaway, although more speculative, is that different emotional outcomes could result from different triggers. For example, privacy breaches of healthcare information could potentially lead to embarrassment, judgment, or a loss of status. App vulnerability could make people feel always on, fettered, or distrusted. Social media risks feelings of manipulation, distraction, betrayal, or anxiety about one's reputation. Spatial intrusions might make people feel ashamed, exposed, or self-filtering. Hacking threats might make folks feel wronged, violated, or paranoid. Cyber-tips, even if intended to be helpful, might make people feel overwhelmed, neglectful, or naïve. And privacy vulnerability regarding government access might make people feel guilty, punished, or lacking in liberty.

Understanding this variation can be vital to help companies connect emotionally in their marketing and messaging strategy around privacy resilience, and to match the great diversity of consumer and data scenarios they face.



**The next few pages unpack the words associated with each of the seven topics.** These antecedents reveal what arouses privacy vulnerability, but there is more to learn about the emotional outcomes that people wish to protect against. We turn to that in the sections to follow.

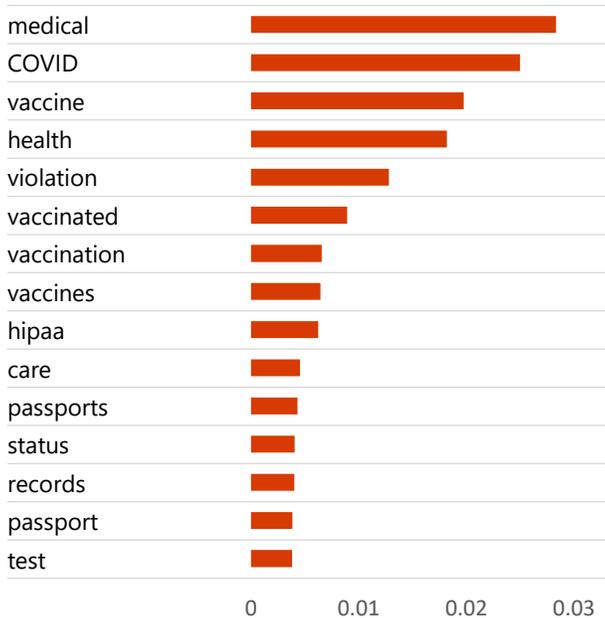
# Topics in online conversations about privacy vulnerability

## 01 / Health & COVID-19

"Say NO to COVID passports it's an invasion of our medical privacy!" (All quotes reflect research participants' views, not those of the authors or their organizations.) This topic exemplified that interference in, and compulsion of behaviors or decisions is a part of the privacy construct to many people. (See Exhibit 3) Posts discussed the resistance to disclose vaccine or exposure status among other health conditions, but they often went on to discuss the impact to work, travel, or business patronage. The lesson here is the close psychological relationship between liberty and privacy, rather than thinking about privacy as merely informational.

### EXHIBIT 3. HEALTH & COVID-19

Probability term belongs to topic

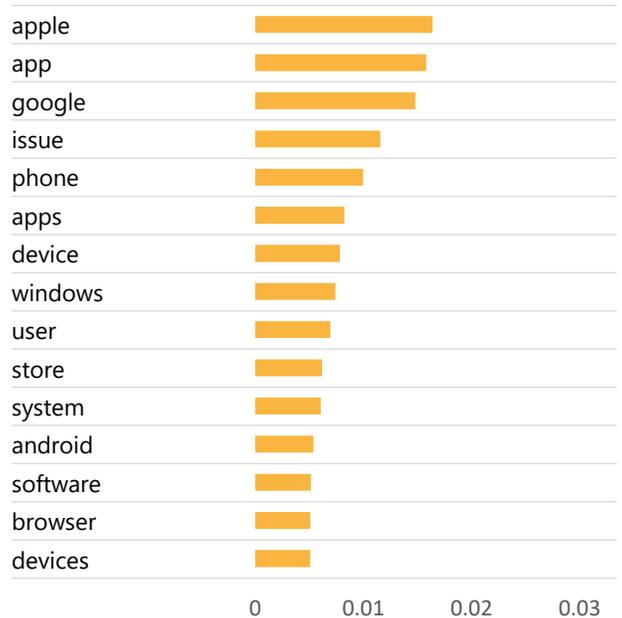


## 02 / Apps & devices

"My GF [girlfriend] can track the exact position of my [car brand] using her [Car Brand] App (Added as an additional key to my car). This is a serious privacy issue." This topic also reflected current events, particularly about prohibiting smartphone apps from passive data collection such as location, search terms, and browsing behavior. (See Exhibit 4) This topic was the most internally diverse, involving a broader variety of words than the others, and it certainly represents the newest forms of privacy concerns.

### EXHIBIT 4. APPS & DEVICES

Probability term belongs to topic



"When I pick up a phone call that I don't know the number, I say, I need to know your name and ID number and what you're doing."

US Consumer

### 03 / Social media

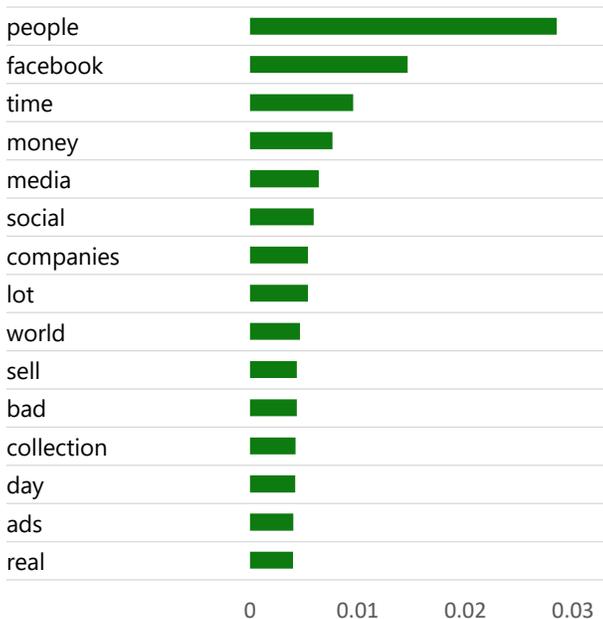
"[Platform] could have been something useful, but it devolved into algorithms aimed towards propaganda and selling user data. This is a serious privacy issue." Not long ago, we might have expected to see this topic dominated by surprisingly sensitive peer-to-peer self-disclosure on social media platforms. But today the topic has shifted to discussing the targeting of misinformation, inappropriate B2B sharing, and manipulative algorithms. (See Exhibit 5) No surprise that it appeared in our analysis, although it is not appreciably more prevalent than the other topics.

### 04 / Presumption of privacy & personal space

"I'm terrified of being on camera. If this was someone taking this picture of me to post on the web, I would feel extremely violated. People do have basic privacy rights." This topic was the most prevalent, and it represented a blend of intrusions into personal space and violations of the presumption of privacy. (See Exhibit 6) Posts in this topic had the highest prevalence of negative sentiment (75% compared to 50% overall). This topic was most directly connected to Westin's (1967) belief that emotional release from the tensions of social life is a fundamental need met by privacy, along with the need to repair and reflect with solitude. Violations of this need appeared to arouse the most acute negative emotionality and resulting behavioral action.

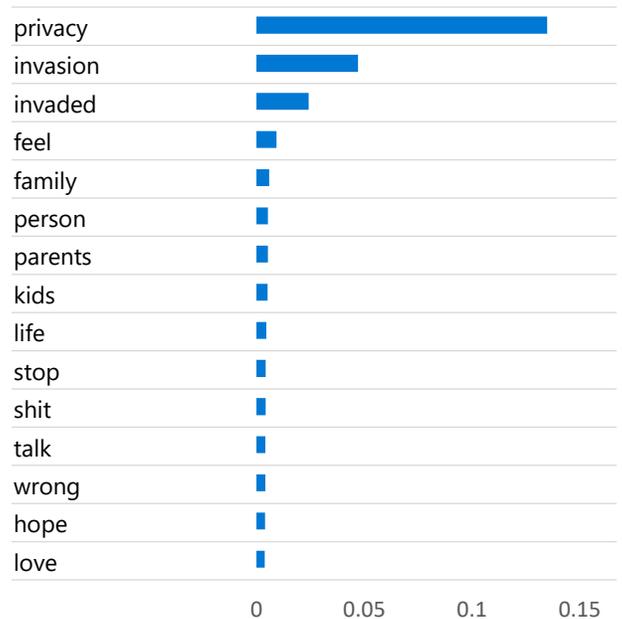
#### EXHIBIT 5. SOCIAL MEDIA

Probability term belongs to topic



#### EXHIBIT 6. PRESUMPTION OF PRIVACY & PERSONAL SPACE

Probability term belongs to topic

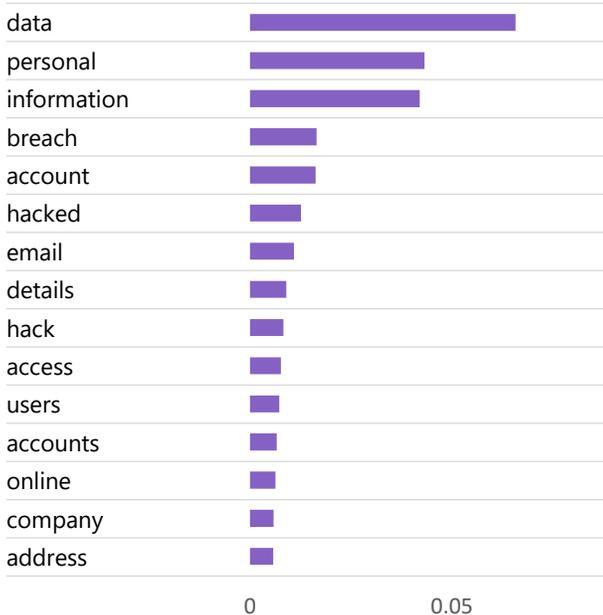


## 05 / Hacking

*"[Airline] suffered a major cyber-attack and the personal data of passengers hacked including credit cards, passport, and other details. Thanks to our regulators for not bringing stricter data and cybersecurity policies!"* This topic demonstrates that privacy violations are felt as a form of theft, and that people can be expected to be concerned about having what is theirs be taken from them. (See Exhibit 7) Regardless whether the hacked information can lead to further financial loss or not (e.g. credit cards versus photos), information is experienced as an extension of the self, and thus protecting it is protecting ourselves. Finally, the hacking topic reminds us that security is necessary to protect privacy, but not sufficient.

### EXHIBIT 7. HACKING

Probability term belongs to topic

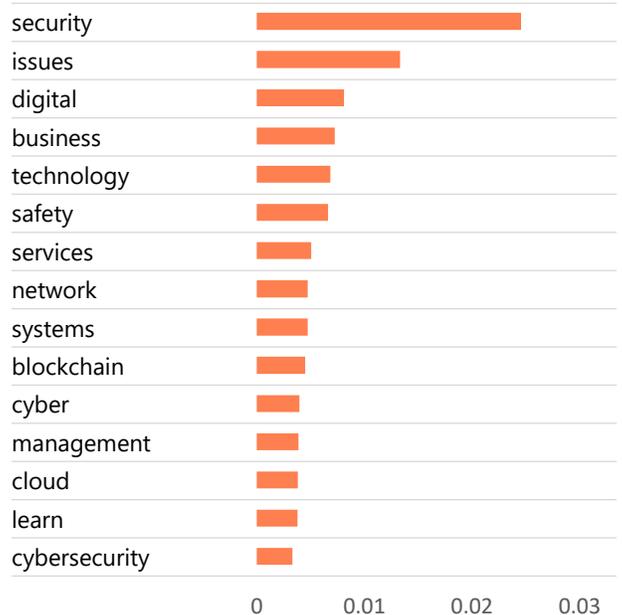


## 06 / Cybersecurity tips

*"I was threatened by a hacker to dox my identity and hack my personal data to the public in exchange for my NFT. We should watch out guys!"* "Doxing," to clarify, is when sensitive or identifying information about a particular individual is published online, typically in a peer-to-peer form and with malicious intent. This topic was characterized by folks' efforts to warn each other about privacy threats like this and to share tips on defending against them. (See Exhibit 8). This topic is the least negative (30% of posts) of the seven, and it represents the constructive flipside of the hacking topic.

### EXHIBIT 8. CYBERSECURITY TIPS

Probability term belongs to topic



**"Hacking is a real thing, it happens. I have had plenty of friends and family who've gotten swindled out of something."**

US Consumer

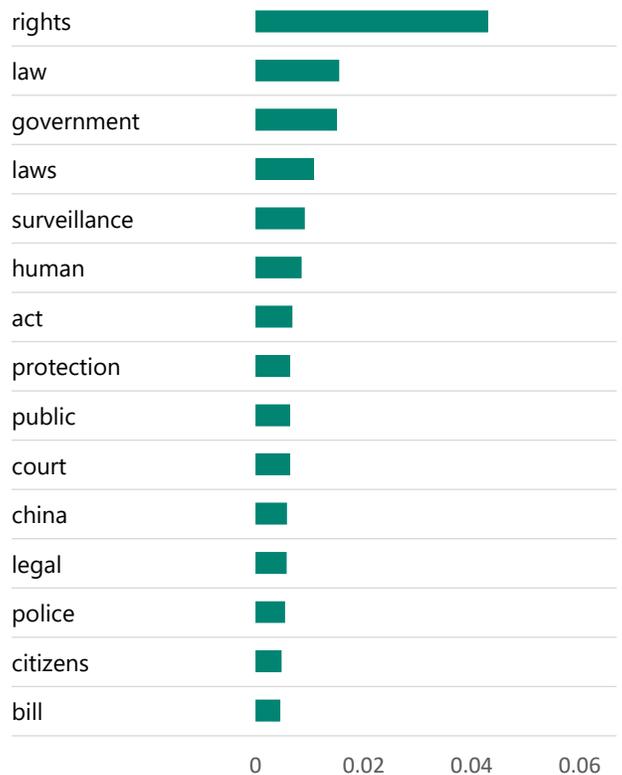
## 07 / Government influence

*"It would be a violation of the 4th amendment but because everyone gives up the data in a way legally defined as legal, and companies collect it in a way that's legal, and sell it in a way that's legal, and governments buy it in a way that's legal, it isn't illegal."* So much of the writing and thinking about privacy historically involves how to limit warrantless search and seizure (Smith & Browne, 2021). Even Westin (1967) pointed out that rights prohibiting torture and self-incrimination arose to protect privacy, because at that time the only way to get information was from the mouths of people. Today the passive surveillance of globally-traversing digital communications can be done at scale without awareness, so this concern remains acute.

**(See Exhibit 9)** The surprise lesson here is that government influence is only one of seven very diverse topics in the concerns that people have for privacy today, and not the most common.

### EXHIBIT 9. GOVERNMENT INFLUENCE

Probability term belongs to topic



# The emotional texture of privacy vulnerability

---

*“Having my identity or financial information stolen would make me feel violated, angry and very worried about the future.”*

---

US Consumer from Hypothesis Group primary research survey



# The emotional texture of privacy vulnerability

In April and May of 2022, we commissioned the agency HYPOTHESIS to field a 20-minute survey in the US and Germany (see detailed methodology in the Appendix). To better understand the emotional texture of privacy vulnerability, we developed a list of concerning outcomes from our literature review, social-media analysis, and qualitative interviews. These purposefully straddled privacy concerns and outcomes in the APCO model frequently used to partition the privacy phenomenon (Antecedents, Privacy Concerns, Outcomes; Smith, Dinev & Xu, 2011).

Our list represented broad emotional outcomes like “feeling betrayed” rather than specific harms such as “the sale of my personal data.”

We asked consumers and privacy pros in the US and Germany to evaluate their most and least important concerns in a MaxDiff trade-off exercise which does not offer the option to say they are all important. US and German respondents were aggregated for maximum generalizability (noteworthy variations are reported where found). We factor-analyzed results and found that responses converged into several facets of privacy vulnerability (in order of importance, they were Victimization, Helplessness, Intrusion, Reputation and Relationship Damage, Legal Compulsion, and Self-impression & self-determination). (See Exhibit 10)

## EXHIBIT 10. CATEGORIES OF DATA PRIVACY CONCERNS (FACTOR ANALYSIS RESULTS)

1 Victimization	2 Helplessness	4 Reputation & relationship Damage	6 Self-impression & self-determination
Fearing identity being stolen	Losing freedoms	Damaging reputation among general public	Being judged out of context
Fearing misuse of private information provided	Losing a sense of control	Limiting future opportunities in work/ school	Losing control of their impression
Risking future loss or theft	Feeling betrayed	Risking future healthcare problems	Altering plans for the future
Risking someone finding my/their private information	Feeling helpless	Compromising my/their relationship with employer	Feeling a loss of places to be alone
Being falsely accused	<b>3 Intrusion</b>	Damaging reputation among peers	Rewriting the story of my/their life
Losing a sense of security	Feeling watched	Impairing relationships	Not appearing to who they strive to be
Having something taken from me/them	Making personal moments public	<b>5 Legal compulsion</b>	Feeling a loss of belonging to a group/community
Feeling violated	Feeling misled	Being investigated	Losing tradition, custom, or heritage
Losing what I've/they've achieved		Being forced to give identification	Feeling compelled to be always “on”
		Being compelled to conform to laws, customs, or values	Being seen as flawed

\*Categories are ranked in order of importance

**EXHIBIT 11. TOP DATA PRIVACY CONCERNS IN 2022 SURVEY IN US  
AND GERMANY (MAXDIFF SCORES)**



Consumers



Privacy Pros

MORE IMPACTFUL

LESS IMPACTFUL

		Consumers	Privacy Pros
Victimization	Fearing my/their identity being stolen	218	164
Victimization	Fearing misuse of the private information I/they provide	192	159
Victimization	Risking future loss or theft	186	129
Victimization	Risking someone finding my/their private information	172	142
Victimization	Being falsely accused	162	102
Victimization	Losing a sense of security	157	148
Victimization	Having something taken from me/them	136	104
Victimization	Feeling violated	135	97
Helplessness	Losing freedoms	129	100
Victimization	Losing what I've/they've achieved	118	99
Helplessness	Losing a sense of control	114	92
Intrusion	Feeling watched	112	85
Legal Compulsion	Being investigated	106	98
Helplessness	Feeling betrayed	101	90
Intrusion	Making personal moments public	97	99
Reputation & Relationship Damage	Damaging reputation among general public	93	127
Helplessness	Feeling helpless	93	85
Reputation & Relationship Damage	Limiting future opportunities in work or school	88	113
Legal Compulsion	Being forced to give identification	85	90
Legal Compulsion	Being compelled to conform to laws, customs, or values	84	103
Reputation & Relationship Damage	Risking future healthcare problems	72	104
Reputation & Relationship Damage	Compromising my/their relationship with employer	71	98
Intrusion	Feeling misled	70	74
Reputation & Relationship Damage	Damaging reputation among peers	64	118
Reputation & Relationship Damage	Impairing relationships	63	85

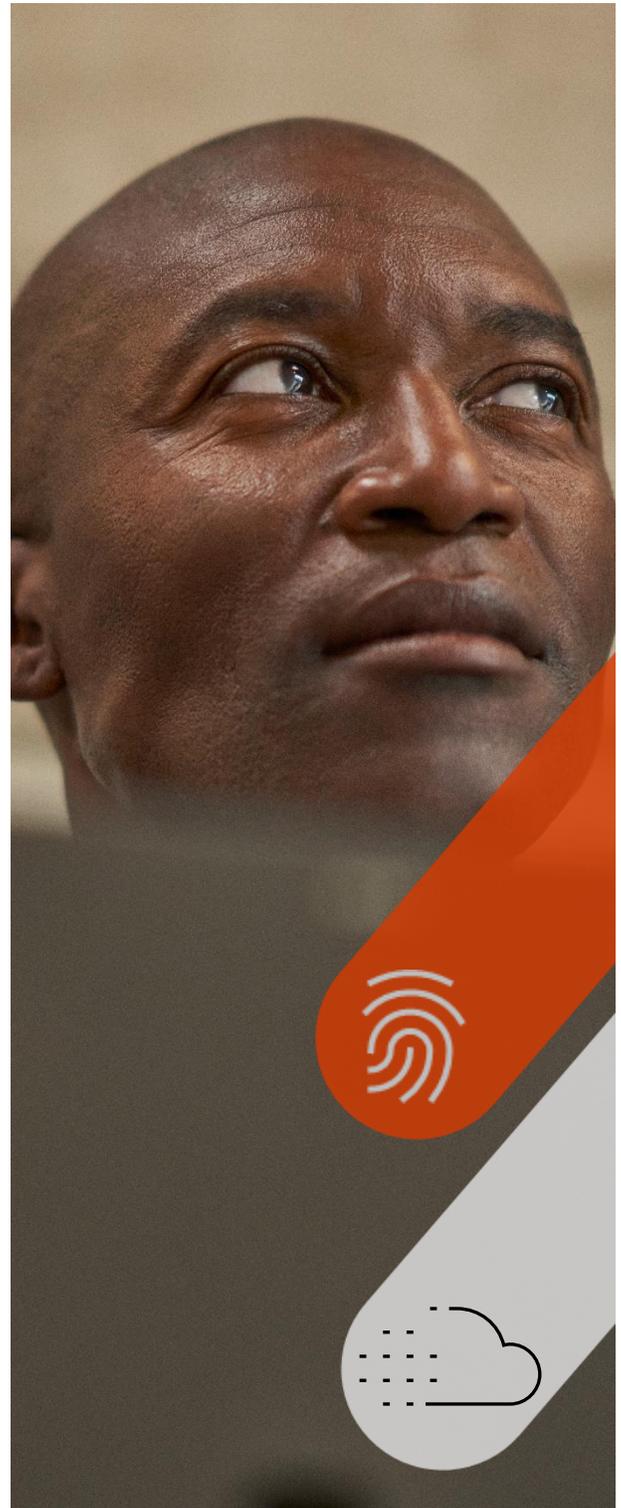
Green shading indicates this item indexes over 110, with 100 as average

It is immediately clear from **Exhibit 11** that *victimization* is the facet of privacy vulnerability that companies must commit to protecting above all others (any data points over 110 indicate that these items are above average importance). Concerns related to the pocketbook — like stolen identities, loss or theft, and data misuse — are top of mind for consumers. This finding is corroborated by research showing that people want their financial information to be protected more rigorously than other types of data (Palmatier & Martin, 2019; Morey, et al., 2015).

It is interesting to note that common commitments that companies make to grant *control* over how data is used and *transparency* in knowing whom companies intentionally share it with — two mainstays of privacy policies and public web-pages — do not address victimization concerns very directly. For companies to inspire privacy resilience, safeguarding personal data and identifying and preventing critical privacy risks are investments to make and commitments to amplify. A top protection respondents demanded was *a sense of security* which is all the more powerful the more broadly it is interpreted.

To further differentiate from competitors in projecting privacy resilience, companies should understand and address the other top themes of *helplessness, reputation and relationship damage, intrusion and legal compulsion*.

(See **Exhibit 11**)





Respondents in our study also signaled a strong need to protect their self-image almost as importantly as their bank accounts. Top concerns like *being falsely accused, losing what I've achieved, damaged reputations*, and even their private information being *found* and *misused* indicate that for many, it's about more than money. It's about owning their futures and living an effective life (see Doss, 2020; Zuboff, 2019).

In fact, privacy pros felt that consumers should be more concerned about *reputation and relationship damage* than they currently are. Privacy pros seemed to understand the risks of damaged reputation among peers and the public, and the resulting risks to future opportunities in work or school more so than consumers did. "Doxing," the malicious and intentional publishing of private information, was a theme in our qualitative interviews. Getting ahead of such harms will set companies apart and help them best serve consumers.

Privacy pros, however, underestimated concerns of *helplessness* among consumers, like losing a sense of control, feeling betrayed, and potentially losing freedoms. When we isolated those consumers who had the most personal exposure to privacy breaches, we found that these same feelings of helplessness, worry, and being taken advantage of only increased.

What emotion words best capture privacy vulnerability? Our survey showed that *violated*, *worried*, *angry*, *powerless*, and of course *vulnerable* top the lists in both the US and Germany. (See Exhibit 12) This insight can help companies identify with how consumers are feeling in their communications. Interestingly, we found that those who were rarely exposed to privacy breaches reported feeling the most *violated* and *angry*, but among those with more frequent exposure, these emotions gave way to feeling *taken advantage of*, *worried*, and *helpless* (US findings). All of these are unpleasant emotional states that consumers will take action to end, and that includes taking their business elsewhere.

In a final look at inspiring privacy resilience, we next asked consumers directly what commitments they need to hear from companies.

**EXHIBIT 12. TOP EMOTION WORDS DESCRIBING PRIVACY CONCERNS AMONG CONSUMERS**

US 	Germany 
<b>Violated</b> (36%)	<b>Worried</b> (28%)
<b>Worried</b> (22%)	<b>Angry</b> (21%)
<b>Angry</b> (22%)	<b>Vulnerable</b> (21%)
<b>Vulnerable</b> (22%)	<b>Powerless</b> (21%)
<b>Taken advantage of</b> (20%)	<b>Helpless</b> (20%)

**“I would feel angry, it would ruin everything that I have worked so hard to have in my life.”**

US Consumer

**“I don’t feel like I have a sense of privacy or control. It makes me feel very vulnerable.”**

US Consumer

# The commitments that foster privacy resilience

# The commitments that foster privacy resilience

Our surveys next asked consumers what they felt companies should commit to protecting. We asked privacy pros parallel questions about what they thought consumers needed to hear. Responses were collected with a simple selection of the top 5 and bottom 5 in the full list of 23.

Here we were able to analyze again whether *transparency* and *control* were the commitments that were most compelling to consumers. We knew from the economic models reported earlier that these reassurances improve business outcomes (Martin et al., 2017, 2020; Chisam et al., 2022). But are there other commitments that are similarly imperative to make?

*Control* was affirmed to be a top commitment that consumers in both US and Germany need to hear from companies. (See Exhibit 13)

Privacy pros underestimated this need in both countries (sharply in the US). Just as people seek to manage whom they form a relationship with via self-disclosure, and what impressions others have of them, they also want to be able to direct and shape the data they entrust to companies.

As important as control, and even more important than transparency, was the need for companies to protect *trust* and a *sense of security* when it comes to consumers' *ownership* of private information. *Transparency* was still high in importance (and is often required by regulations) as both consumers and privacy pros agreed. But a key finding for public-facing messaging about privacy protection is that companies must also bolster the security that consumers feel when trusting them with their data and reduce the sense of vulnerability.

**"I expect for data protection, to be able to control what information I have access to and what I delete."**

US Consumer

**"It's a matter of putting people in a bad position, ruining your reputation, losing that customer, which means that it's going to be a financial impact. And again, you're going to kill your brand."**

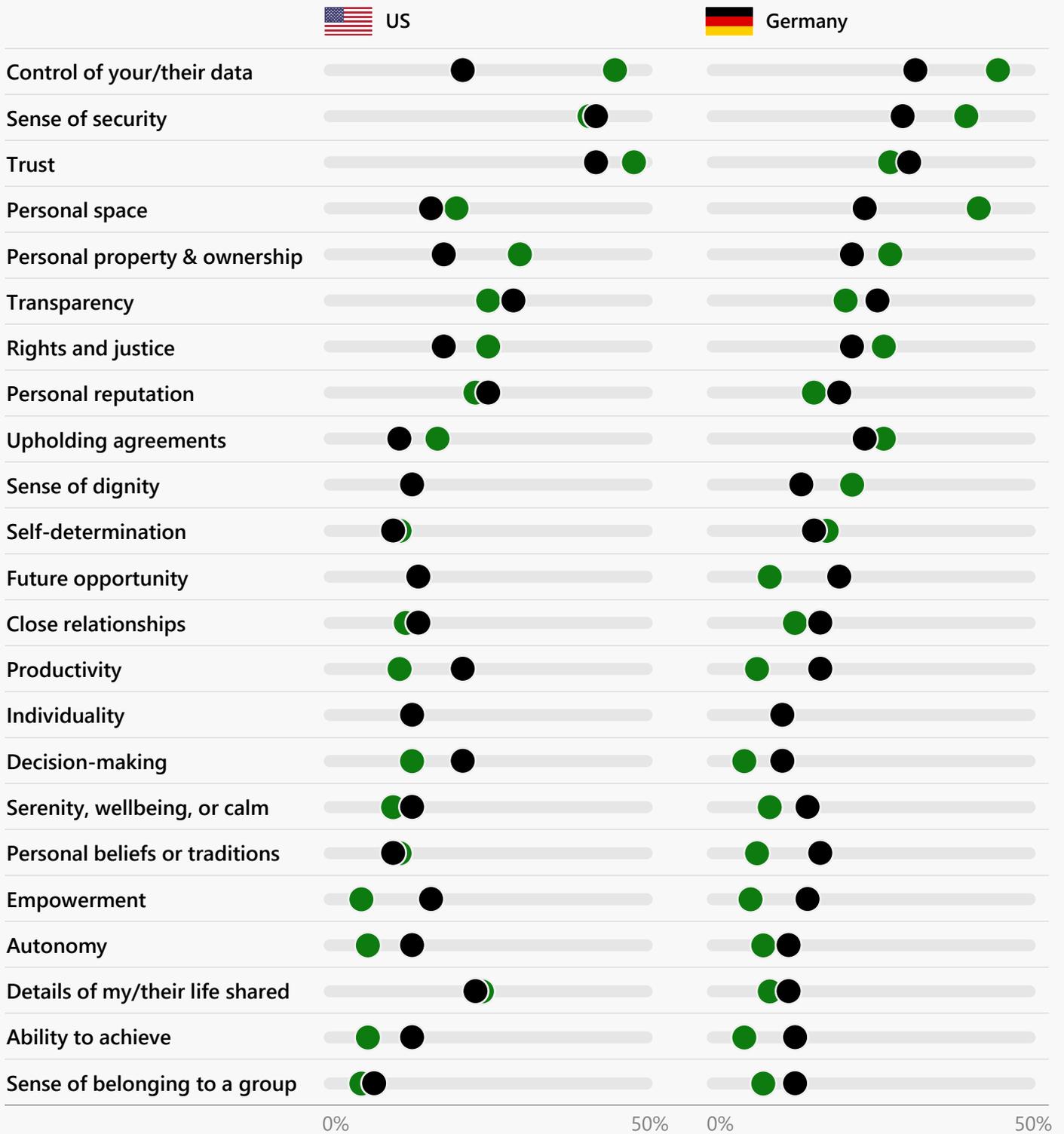
US Privacy Pro

\*See full list of commitments for data privacy on page 40

# Exhibit footnotes



## EXHIBIT 13. DESIRED COMMITMENTS FOR DATA PRIVACY

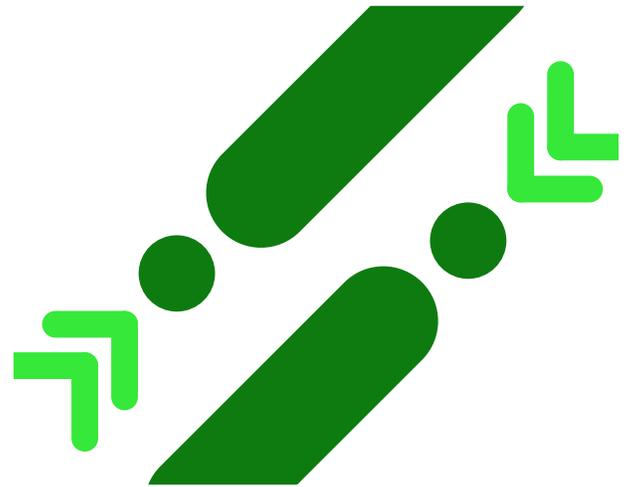


The need to protect personal *reputation* (US) and *dignity* (Germany) was also in a similar tier as the need for *transparency*. Consumers and privacy pros were aligned on these commitments. Somewhat more so than consumers, privacy pros acknowledged their responsibility to protect *decision-making*, *empowerment*, *productivity*, and *achievement* in handling and processing consumers' private information. Broadly, this pattern suggested that privacy pros fall short in understanding how much consumers need control and security protections, while perhaps seeing risks consumers do not yet in terms of protecting reputation and dignity.

The most striking regional difference was that in Germany, consumers also need to hear commitments to protect *personal spaces*, a top need that was also the one most sharply underestimated by German privacy pros. (See Exhibit 14) This might be attributable to the still salient history of Stasi home surveillance by the former German Democratic Republic before its end in 1990, which many feel is still essential to understanding privacy concerns in German culture (Smith & Browne, 2021).

A final theme worth noting is how much consumers need *trust*, *upholding agreements*, and protecting privacy *rights & justice*. Further exploration is needed, but these needs seem related to limiting the use of private information to the purpose made known at the time it was provided. Privacy thus seems to be an influence in demonstrating the face validity of a business exchange, that is, the benefits that were provided in return for the costs.

When this breaks down, and when other uses and other parties including government enter into the relationship, trust suffers. And savvy companies know that trust is earned by the spoonful and lost by the bucket.



**Summarizing:** Companies who want to connect empathically in marketing messages related to privacy and differentiate from competitors, should deepen their commitment to granting consumers control to see, modify, delete or transfer their data. They should rethink undifferentiated and unsupported promises of transparency, putting as much emphasis on cultivating trust, reducing consumers' sense of privacy vulnerability, and replacing it with clear protections of ownership and due process. There are larger reputational, and dignity needs at play in privacy resilience, which companies can speak to only after they prevent identity theft and all forms of financial loss and intrusion into personal spaces.

# Privacy resilience is a differentiator

# Privacy resilience is a differentiator

Will connecting empathically with consumers and inspiring privacy resilience help companies differentiate? Published modeling studies reported earlier suggest that reducing privacy vulnerability positively influences consumers and investors. Did our survey respondents also feel it could set companies apart?

**A supermajority of consumers (70%) affirmed directly that they prefer to use companies that “communicate that they understand my privacy concerns.”** (See Exhibit 14) About half or more of consumers further reported that how a company handles their online privacy and data security has “helped convince me to use their product, service, or apps” and “helped set them apart from competitors.”

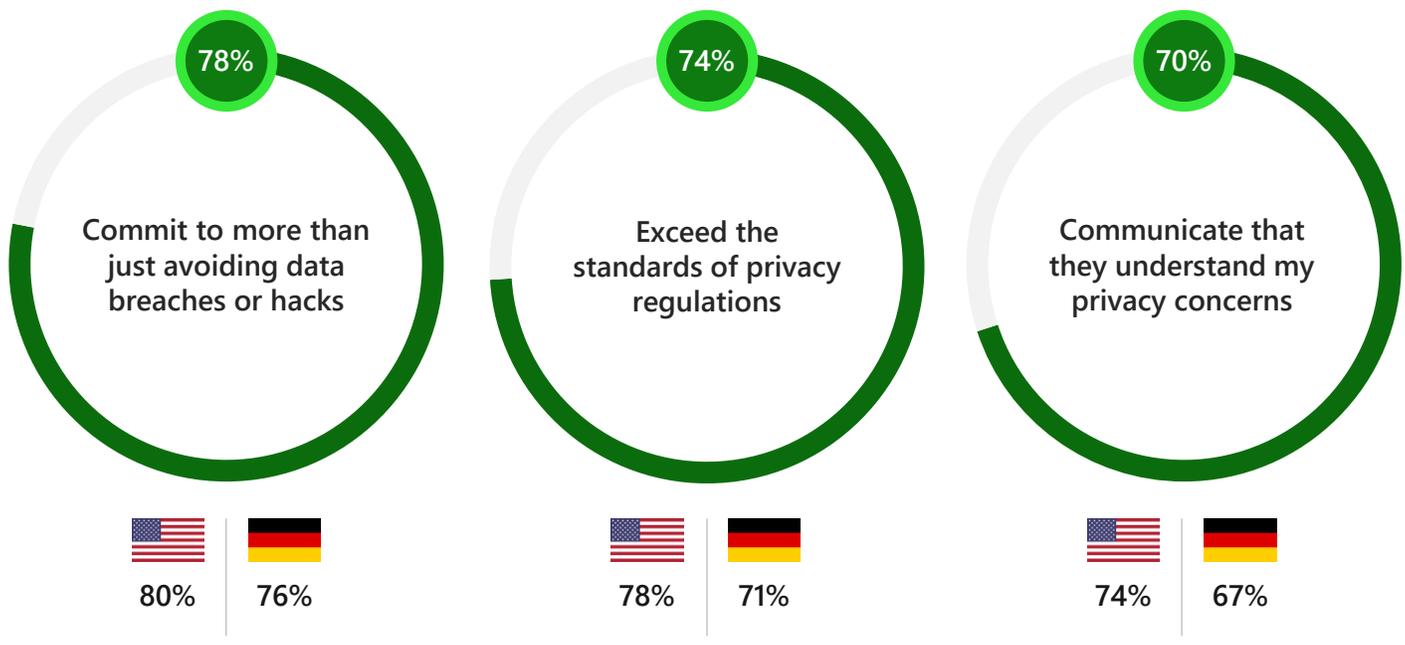
The downside was also true, about half of the consumers (46%) reported that they were deterred from engaging with a company over how it handles their online privacy and data security.

Interestingly, the need for companies to address their concerns was equally as powerful in consumers’ opinions as was totally avoiding a data breach or hack. Affirming this directly, 78% of consumers preferred companies that “commit to more than just avoiding data breaches or hacks.” In addition, 74% of consumers preferred companies that “exceed the standards of privacy regulations.”

EXHIBIT 14. AGREEMENT WITH PRIVACY STATEMENTS ABOUT DIFFERENTIATION



Consumers



\*All reports of agreement or affirmation report the “top-2 box” percentages, that is somewhat + strongly agree

All this suggests that companies' investments in meeting or exceeding regulations could germinate compelling and differentiating marketing messages.

Privacy pros need little convincing that privacy is a differentiator, the survey suggests. (See Exhibit 15) 90% of commercial privacy pros affirmed that their company's stance on online privacy and data security "has helped us acquire B2C clients." In addition, privacy pros agreed their privacy stance had helped them acquire "B2B clients" (88%) as well as "key partners" (89%).

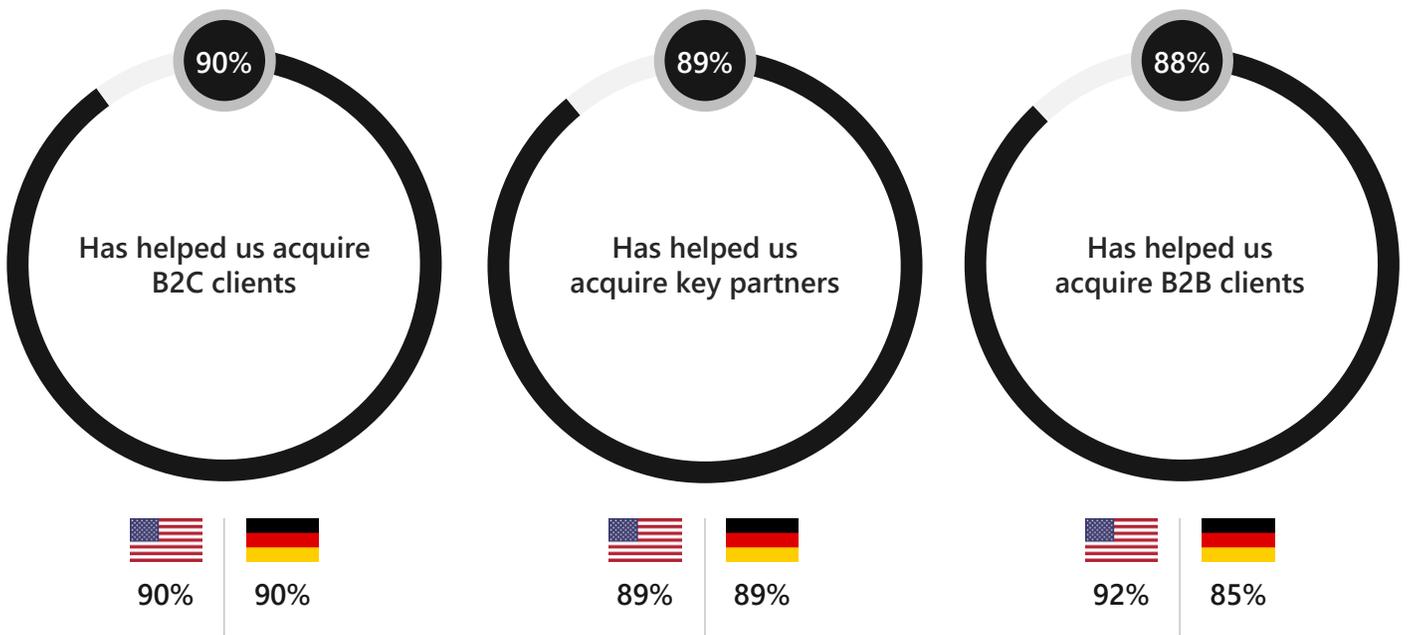
**"Putting a personal aspect to privacy and letting consumers know that it's our core value is a key piece when communicating to our end user."**

US Privacy Pro

EXHIBIT 15. IMPACT OF PRIVACY ON BUSINESS RELATIONSHIPS



Privacy pros



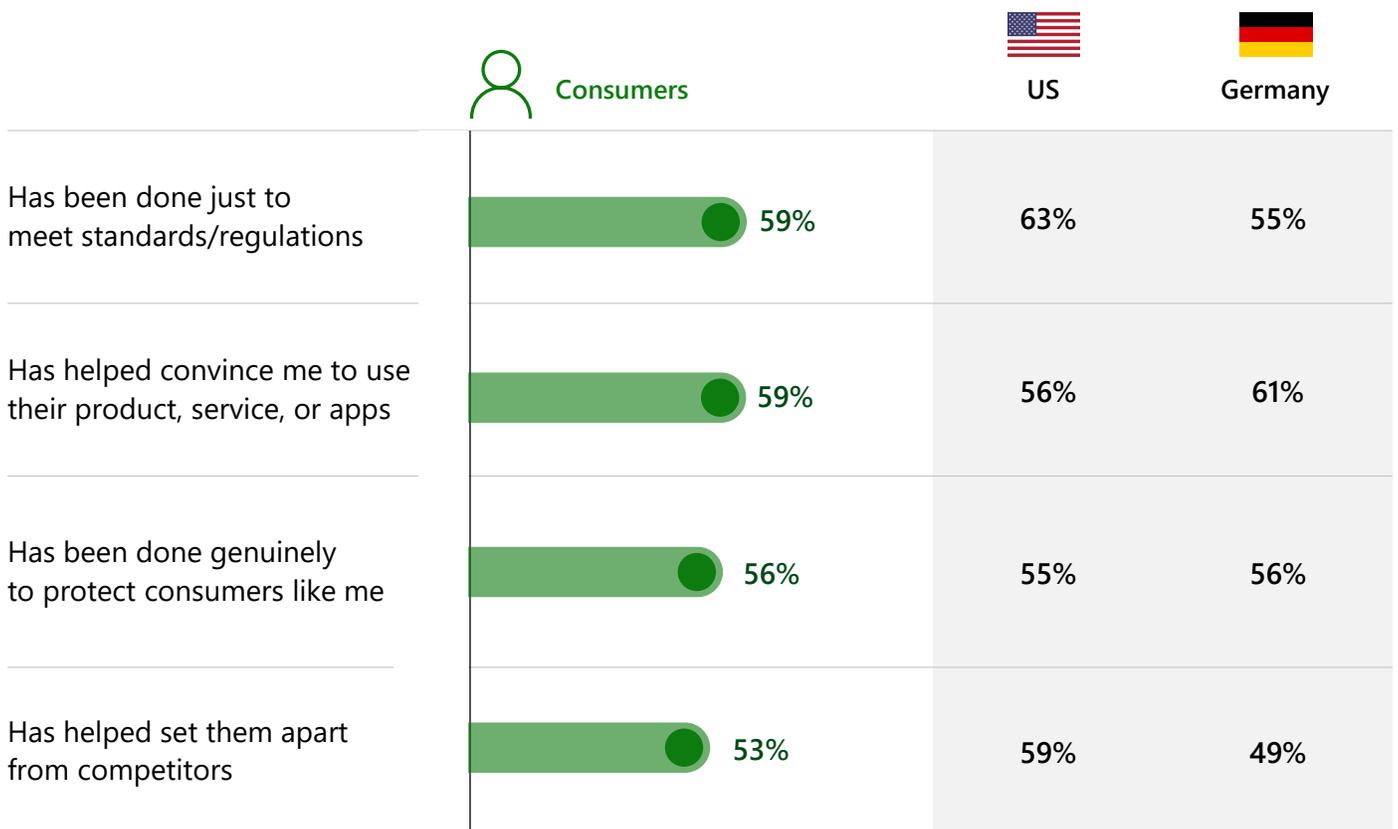
\*All reports of agreement or affirmation report the "top-2 box" percentages, that is somewhat + strongly agree

The road is clear — companies stand to gain a lot by reducing privacy vulnerability and elevating privacy resilience — but that doesn't mean that authentic messaging and earning trust will be easy. A cautionary note was also sounded by the consumers who took our survey. Over half of consumers perceive that how companies handle their private data “has been done just to meet standards and regulations.” (See Exhibit 16) Even though 93% of privacy pros felt their organizations “make it a priority to authentically

uphold our company's mission and values when it comes to our consumers online privacy,” only a little more than half of consumers (56%) felt companies' privacy handling “has been done genuinely to protect consumers like me.”

Business-specific and culturally sensitive privacy messaging will need to be fashioned and allowed to change dynamically across consumers' lifecycles. But an empathic connection will only build trust if it is authentic.

**EXHIBIT 16. TOP DATA PRIVACY DIFFERENTIATORS AMONG CONSUMERS\***



\*All reports of agreement or affirmation report the “Top 2 Box” percentages, that is somewhat + strongly agree

# Move your company up the privacy resilience spectrum

# Move your company up the privacy resilience spectrum

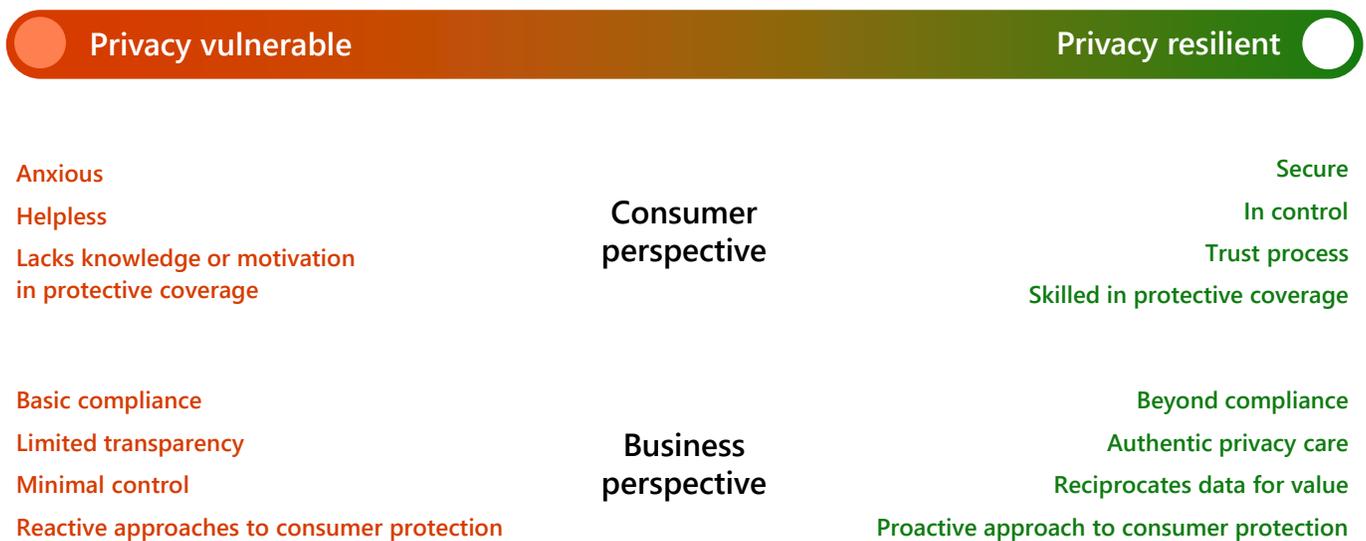
We've seen that when done authentically, reducing the subjective sense of privacy vulnerability among all those who entrust your company with their data is imperative to business success and standing apart from competitors. The survey data presented here help empathize with the triggers and emotions your stakeholders feel, and the commitments they need to hear. (See Exhibit 17)

Privacy vulnerability is more than a breakthrough psychological insight into consumer sentiment. It also describes companies in which data overexposure, hoarding, and risky transfers are common, whether due to a lack of awareness or a lack of accountability. These risky practices threaten trusted data owners with the harms they fear most.

Privacy vulnerability also describes companies that fulfill data-subject requests unconvincingly, giving only a "best effort" to show regulators. And privacy vulnerability describes companies who don't believe that they can lose consumers to competitors.

On the other end of the spectrum, privacy resilient companies inspire a sense privacy resilience in their consumers. How? The research we reviewed from the University of Washington Sales and Marketing Institute (Chisam, et al., 2022), recommended companies start by storing data in the cloud, where providers like Microsoft can confer our rigorous security, compliance, and privacy standards, patterning to its industry and local laws. This saves companies from

## EXHIBIT 17. THE PRIVACY VULNERABILITY-RESILIENCE SPECTRUM



attempting to re-create this level of protection, and it comforts consumers and stakeholders

Companies then layer on a privacy management solution like Microsoft Priva to proactively protect against risks and respond quickly and reassuringly to those wishing to see or access their data. With the time they save on these and other capabilities, they build a human-centered privacy process and empower smarter data-handling policies. In training their workforce, they leverage the profound whys discussed here to inspire authentic participation in privacy protection.

In every touchpoint and communication this ecosystem requires, privacy resilient companies connect emotionally and show empathy behind their investments. They let consumers, clients, partners, and employees know that they understand their concerns and are investing ultimately in trust, control, and a reputation for privacy resilience.

In time, everyone who trusts data to privacy-resilient companies learn that they can be present in the moment and benefit from real value, because their pasts and their futures are protected from influences outside their control.

**“Our corporate culture reflects our values as a trusted partner for our consumers. Our reputation is based on trust.”**

DE Privacy Pro

**“It's not easy, but I think we should communicate that we're doing this because we believe in it, and we believe it's the right thing.”**

US Privacy Pro

# Scenarios that evoke privacy vulnerability or privacy resilience

## Online Food Delivery Apps

Online food delivery platforms are a popular choice for consumers, offering a convenient way to order from a wide array of restaurants with a single tap of their cell phones, often with discounts. Consumers benefit from this convenience, but their privacy vulnerability can be triggered by sharing personal information (e.g., names, contact numbers, physical addresses, identifying information, and financial information). Restaurant owners themselves feel vulnerable to unauthorized theft or access by hackers of this data during transfer or in storage. Both parties risk financial and reputational harm, which can be alleviated by a privacy resilient workplace that minimizes the risk of a breach.

## Financial Data Breach

In addition to storing and managing money, banks store multiple forms of data and predictive models. Financial data loss (e.g., accidents, hacking) can have real and far-reaching consequences. Consumers feel vulnerable when a bank experiences a cyber-attack that leads to a financial data breach, especially when there is a lag between when the attack was discovered and when it was stopped. Even in instances where login information or social security numbers are not compromised but names, email, and phone numbers are, account holders are vulnerable to increased risk of future phishing attacks. Proper security and privacy risk management can help banks project resilience against cyber attacks like this and set a bank apart.

## Geofencing and Propensity Models

Imagine a double-income couple in the UK books a hotel in Mexico for themselves and their child to take a vacation. After checking in and learning the amenities, the couple takes advantage of a hotel-run child-care services that collects basic health information. The couple picks up the child later without incident, but through the use of geofencing and location awareness, the hotel data records the couple's visit to the bar and the pool in the interim. The couple accepts the privacy policy governing this experience, but they may be confused whether GDPR applies. Enriched data sets from such scenarios can help the hotel provide delightfully tailored services, but the family may wish to know and shape this story to minimize their vulnerability and reputational risk.

## HIPAA Violations

There are many ways medical personnel can accidentally or intentionally commit HIPAA violations. It is not unheard of that healthcare providers inappropriately access the personal health information of friends and family, especially when that information is surprising or revises impressions about known others (e.g. mental health services, reproductive care). Privacy resilient healthcare providers train their staff to understand it's about more than regulatory compliance, it's about minimizing risks of relationship and reputational harm as well as the feelings of vulnerability that might make health concerns go unaddressed. They empathically communicate the resilience of their platforms, policies, and people in meeting patient needs.

# Inspiring the study of privacy psychology

# Inspiring the study of privacy psychology

Historically, designers and marketers in business as well as human-rights advocates in law have looked to academic psychology and other social sciences to understand and align with people emotionally and authentically. Indeed, the 1954 Brown vs. Board of Education ruling that desegregated US schools was informed by a psychological study of how children perceive Black and White dolls (Clark & Clark, 1939).

But when we look for the psychology of privacy, we find a surprising gap. In 1977, Stephen T. Margulis noted that academic psychology had neglected the topic of privacy despite calls for research by Westin (1967) before him. This is a surprise given that social psychology originated with understanding the Holocaust and it grew to maturity during the Stasi surveillance in East Germany during the Cold War. Adjacent theories around gossip, self-disclosure, and impression-management come close, but none of them shed sufficient light on the cognitive, emotional, and identity-based processes that are activated with the threat of a privacy breach.

Shockingly, over 25 years later, Margulis repeated in 2003 that "there continues to be relative indifference to privacy, as a theoretical or research interest, among psychologists in general." A 2019 literature review by Stuart, Bandara and Levine again confirmed that, "you might expect that it would be a key feature of interest for psychologists. However, psychology has historically paid little attention to privacy."

Microsoft's Chief Legal Officer and President Brad Smith calls privacy "one of the great human rights causes of our time." Taking up this cause is strongly aided by a deep appreciation for the human needs that privacy serves and the human toll an absence of privacy takes. To teach us what we are protecting, academic psychology can no longer remain absent from this critical conversation.

Without rigorous social science, public discourse may continue to be distracted by unclear and misleading notions such as the **privacy paradox**. A surface understanding about why consumers verbally prioritize privacy but still share data and fail to adjust app settings can be mischaracterized by popular press and lure business into the false sense that privacy doesn't matter to their customers.



Apparent paradoxes rarely stand up to deeper theoretical investigation. Marketing and retail scholars are beginning to puncture the privacy paradox (see e.g. Martin, 2020; Auxier, Bartoletti & Jarvis, 2021), and in unpublished theses and dissertations, psychology students are offering their own explanations. Promising leads are found in *social exchange theory* (King, 2018), and work on the *personalization* promise (Schwartz, 2019), as well as the *theory of planned behavior* (Saeri, Ogilvie, La Macchia, Smith, & Louis, 2014). People appear willing to trade privacy for value, to take action with increased knowledge and changing norms, and to share personal information to elevate intimacy and trust in carefully selected relationships (business or personal). Historic abuses of privacy have generally been done to compel conformity (to law, custom, and speech), so today's promise of digital experiences tailored to individual uniqueness sparks a very different calculus.

People's selective trust in sharing personal data with businesses is almost certainly dependent on moderating circumstances, and thus entirely logical and unparadoxical. In our surveys, half of US consumers (53%) and slightly fewer German consumers (41%) affirmed that "I share my personal identifying information even though protecting my data is important." What might explain mismatches between privacy attitudes and privacy behaviors?



It could be anything from cognitive biases (framing effects in surveys vs. user experiences), learning curves (what privacy settings to adjust), personality traits (individual differences in privacy concern), cost-benefit analyses (perception of authentic value or tailoring returned for data), or social dynamics (sharing with trusted others reinforces trust and intimacy).

Sorting that out awaits students of psychology, who, in addition, can also offer definitions of privacy that help the world take a more holistic and humanistic view of it. The best definitions will draw attention to both the proximal and ultimate forces affecting privacy, that is, both its experiential causes and effects, as well as the developmental, evolutionary, and even existential needs that it serves.

According to Margulis (1977; 1974), *"Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability."* This definition re-affirms the proximal importance of vulnerability, as well as the ultimate importance of self-determination. Wolfe and Laufer (1974) added that in common discourse, spatial aspects of privacy such as being alone and controlling access was also core to the construct. We too, found personal spaces to be a theme in today's social conversations, and a strong emphasis in German culture.

If Margulis defined what privacy is, Westin's (1967) theory defines why it is important. He emphasized an emotional release from social life, and a space for self-evaluation and moral contemplation that was crucial to growth and risk-taking. The more we learn about the needs that privacy serves, the higher we will likely climb Maslow's hierarchy (1954), finding that beyond safety and security needs, privacy is essential to relationships, achievement, and our sense of agency in pursuing our life stories (see also Schwartz, 1968).

The best modern definition of privacy we found pulls all of this together. It comes from Doss (2020) who defines privacy as *"a wide range of social values and individual prerogatives, such as the ability to control who knows what information about us, and to limit intrusions into the solitude of our lives. Privacy certainly encompasses these things, but it also implies a great deal more. Privacy is intrinsic to individual dignity and our sense of personhood, to our ability to live as unique beings. Privacy allows us to test our ideas, to live without undue scrutiny; it lets us choose our relationships, overcome our pasts, and direct our future – and change our minds and our behavior over time."*

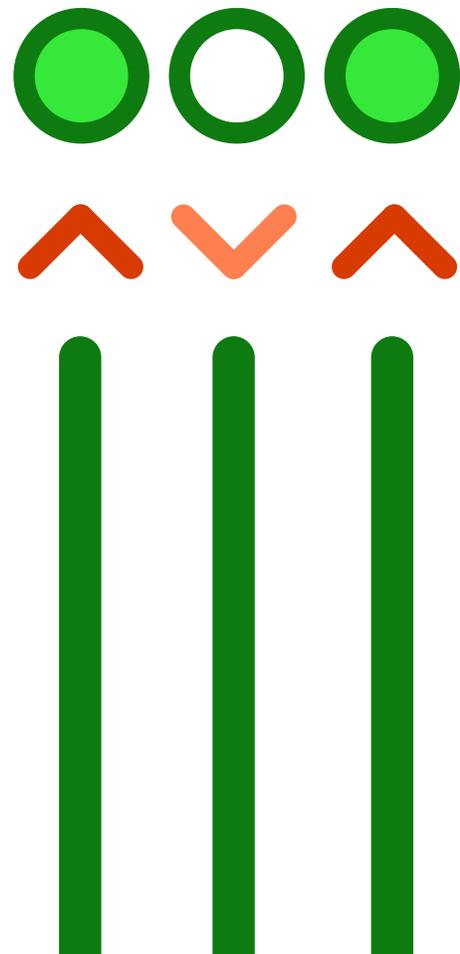
Doss came to this humanistic, empathic view as the Associate General Counsel for Intelligence Law with the National Security Agency. This is a reminder to psychology students who enter this field to build on what is already known about the privacy ecosystem. The social circumstances that trigger privacy

reactions (including transactional, observed, and predicted data types) must be understood because they likely foster qualitatively different privacy concerns (about e.g., security, relationships, reputation), which are in turn centered around different real or imagined harmful outcomes (fraud, family identity theft, doxing). Students should also incorporate into their applied and theoretical models the different roles identified by GDPR law (data subject, data owner/controller, and data processor), as well as different organizational entities such as consumers, regulators, businesses, advertisers, and platform providers.

But once that landscape is mapped and psychology has raised our appreciation about the human needs that we are protecting, there are many specific dynamics in need of investigation.

For example, Kasper (2015) argues that humans experience privacy more acutely when it is lost than when it is gained. In psychological terms, privacy may be inherently a form of negative punishment or loss aversion - a violated assumption rather than a welcomed enhancement. We do not yet know whether this is inherent to the construct across time and across cultures, or whether it reflects US culture at this point in history, but answers are needed to help spread privacy resilience.

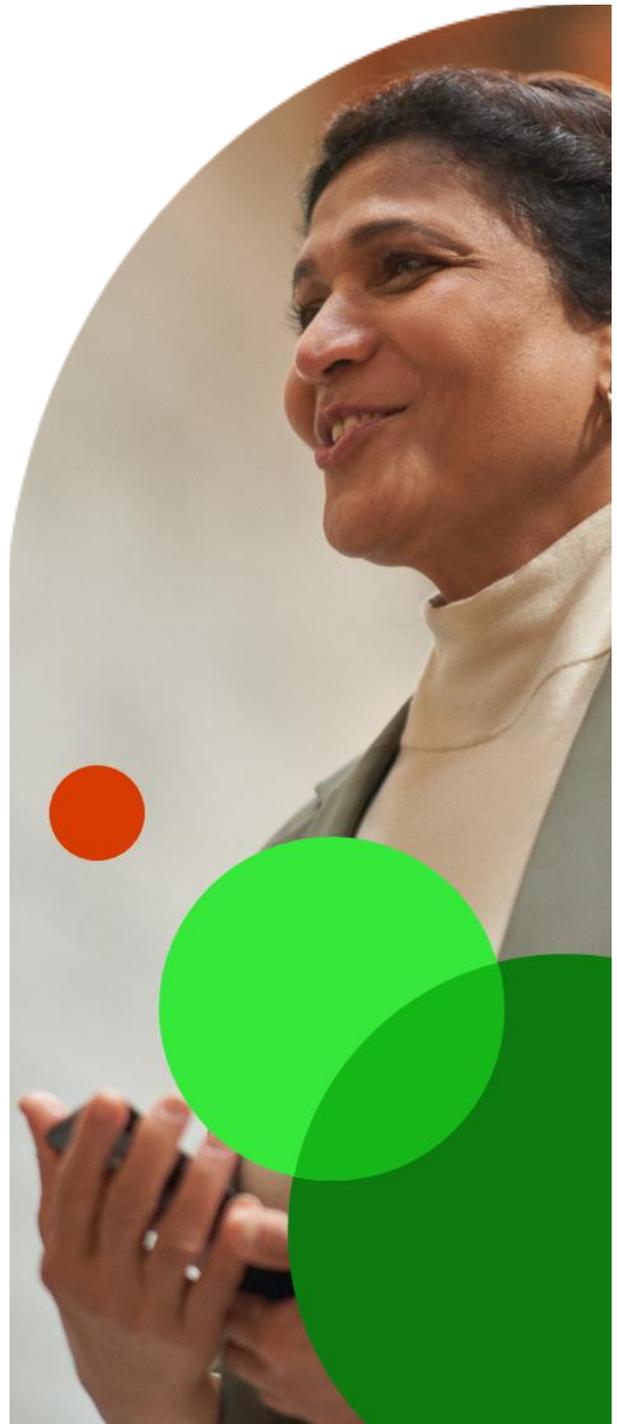
Modern research on privacy must also go beyond scenarios in which information is consciously shared. It must cover observations and predictions made without awareness. This is because today's private information consists of far more than what is knowingly shared in checkouts or other transactions. It includes passive collection of behavioral surplus



(or “digital exhaust,” Morey et al., 2015), such as media consumption and shopping dwell times, or profile information scraped outside of awareness, and even algorithmic propensity predictions about what consumers will buy, watch, vote for, and share with others. Many companies maintain detailed impressions of individuals that the owners may wish to understand and shape in a desire to be seen as they see themselves. But we would first need to be granted access to this “algorithmic self” that exists in the databases of business and government.

For indeed, understanding privacy psychology is a step toward a still greater end - spreading privacy resilience. Laws are being passed around the world granting new rights to be forgotten, to have choice over which organizations we enter relationships with via our data, and to be seen as we wish to be seen. These rights will need to be exercised to retain the dignity and personhood that Doss spoke of, to live as unique beings, and to direct our futures. Microsoft is committed to helping business and enterprise to uphold these rights, just as we uphold them with our own customers. Microsoft exists to empower every person and organization on the planet to achieve more, and ensuring privacy is crucial to that mission.

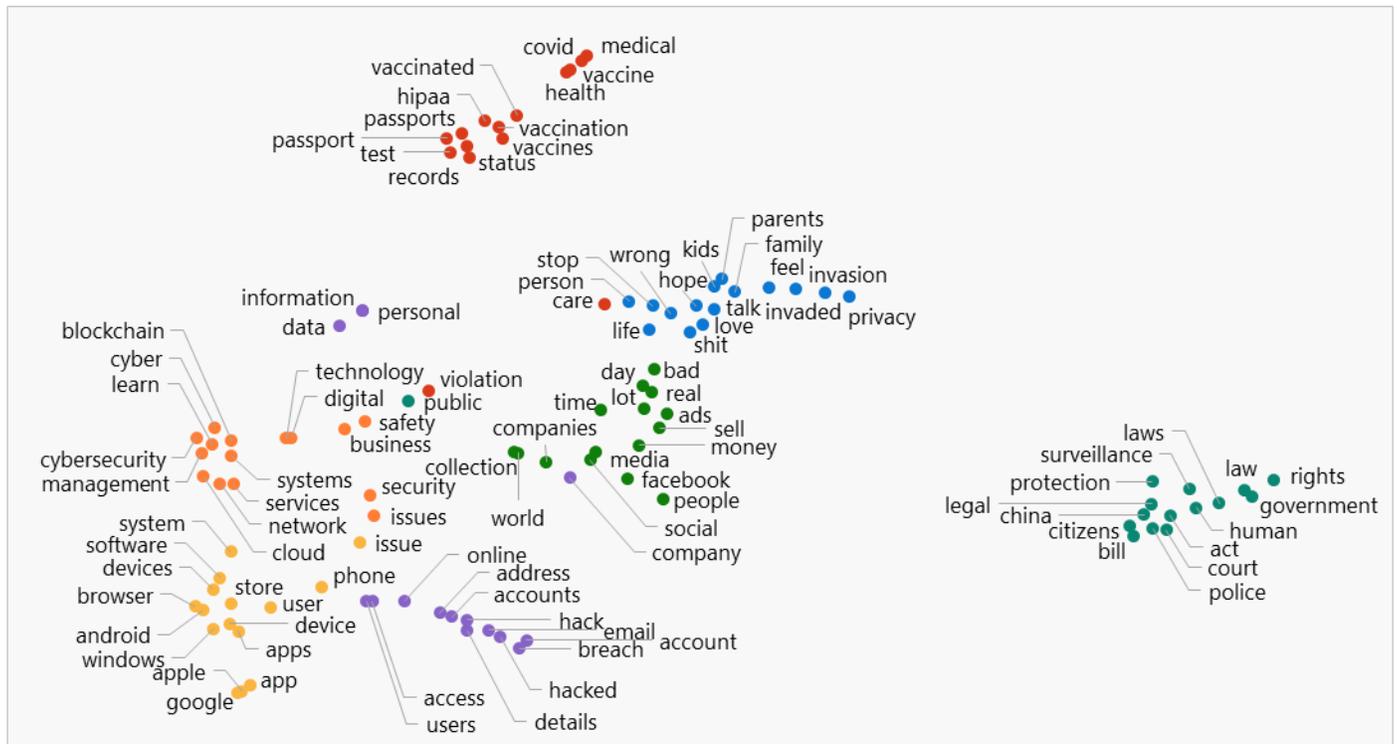
We are reading with great interest student theses and dissertations on the psychology of privacy. We invite more scholars to come into this conversation and continue this crucial work.



# Endnotes

## Actual data map shown from page 14

EXHIBIT 2. TOP DATA VULNERABILITY TOPICS EXPRESSED IN SOCIAL MEDIA (t-SNE MAP 2021)



[Return to page 15 in document](#)

## Social conversation analysis

Partnering with SPRINKLR and the agency SHARE Creative, we queried 412,511 English language posts published globally between 2/16/2021 and 2/15/2022, mainly from the platforms of Twitter, Facebook, Instagram, and Reddit, but also from smaller forums. We structured our query specifically to pull privacy concerns by looking for posts where privacy words appeared near to negative words or anxiety-referencing words, or alternatively near to words like “Orwell,” “Big Brother,” or “creepy” that are mentioned often in our qualitative research on privacy.

From the initial volume of 472,480 posts, we excluded verbatim retweets, known spam accounts, private messages, owned media, branded accounts, global media, and press publications, so as to best represent original conversations among unaffiliated consumers. Sentiment analysis confirmed that concerns dominated the remaining sample, 50% of which were negative in sentiment and under 10% were positive (40% being neutral). The full query structure is sharable upon request.

Latent Dirichlet Allocation (LDA) was used to derive the common topics found in discussions of privacy concerns. LDA is a topic model algorithm commonly used in natural language processing. It statistically analyzes at scale how often words appear in different topics and how common the topics are across the posts. LDA was appropriate here since we did not know and did not wish to define the topics a priori.

Exhibit 2 shows a t-stochastic neighbor embedding (t-SNE) map, which is a dimension reduction technique for visualizing high dimension data. The first axis is defined by identifying the two most probabilistically different terms and placing them at either end of the vertical axis, and then repeating the process for the next set of dissimilar words (“medical” and “google”) to create a second horizontal axis. The remaining topics are plotted revealing clusters.

Exhibits 3-9 shows the LDA probabilities that the words appear in each topic

## Survey research

In April & May of 2022, we partnered with the agency HYPOTHESIS to field a 20-minute survey in the US and Germany. In the US, 206 consumers and 149 privacy pros participated, and in Germany, 233 consumers and 165 privacy pros participated. Consumers were 18-64 years old, census balanced for age, gender, and region, with a natural fall-out in income, education, ethnicity and other key demographics. We also assessed their early or late tech-adoption attitudes. Privacy pros were from companies of 500+ employees in the US (36% over 5,000) or 300+ in Germany (29% over 5,000), who affirmed significant or sole influence over organizational decisions about “data privacy management,” 58% of which were C-Suite or top leadership, and 26% reported to top leadership. Qualitative interviews were conducted to listen to extended remarks and inform the lines of inquiry in the survey.

Exhibits included show responses to the question, “Of the following online privacy and data security considerations, which do you feel are most and least concerning to [you {consumers} | your consumers {privacy pros}].” The prompts were intentionally written to represent emotional concerns and outcomes, rather than situational antecedent triggers. Responses were gathered using a “MaxDiff” approach, which is a commonly used choice decision model where prompts are shown in multiple batches of 4-5 and respondents indicate the “most important” and “least important” concern in each batch, yielding the utility scores shown here. Minor pronoun and wording variations ensured consumers could answer about themselves and privacy pros could answer about their consumers, allowing us to compare audiences. The utilities were factor-analyzed using principal-components factor analysis to yield the categories shown here. Factor labels should be taken as descriptive only and certainly pondered more deeply.

Another Exhibit shows responses to the question, “How does the possibility of a severe data privacy incident (e.g., data breaches, identity theft, online surveillance) happening to you make you feel? (Please select up to 3).” We isolated respondents with more or less personal exposure to privacy breaches by performing a median-split on the question “When it comes to [you {consumers} | your consumers {privacy pros}] online privacy and data security, how regularly do you encounter data privacy incidents (e.g., data breaches, compliance issue, risk management issue)? (Please select one response).” Those with less frequent personal exposure answered, “once or twice a year” or less frequently including “I’ve never encountered a data privacy incident.” Those with more personal exposure answered “once every few months” or more frequently.

- Auxier, B., Bartoletti, I., & Jarvis, D. (2021, June 29). *The consumer data privacy paradox: Real or not?* Deloitte.
- Brough, A.R., & Martin, K.D. (2020). Critical roles of knowledge and motivation in privacy research. *Current Opinion in Psychology*, 2020(31), 11-15.
- Chisam, N., Germann, R., and Palmatier, R.W. (2022). Data privacy regulation: Effects on firm performance. Unpublished University of Washington Working Paper, (22-101).
- Doss, A. F. (2020). *Cyber Privacy: Who Has Your Data and Why You Should Care*. BenBella Books.
- Evans, D.C. (2017). *Bottlenecks: Aligning UX design with user psychology*. Apress.
- Kasper, D.V. (2005). The evolution (or devolution) of privacy. *Sociological Forum*, 1(20), 69-92.
- King, J. (2018). Privacy, disclosure, and social exchange theory. Unpublished doctoral dissertation. University of California, Berkeley, 2018. <https://escholarship.org/uc/item/5hw5w5c1>
- Margulis S.T. (1977). Conceptions of privacy: current status and next steps. *Journal of Social Issues* 33(3), 5-21.
- Margulis, S.T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues*, 59(2), 243-261.
- Margulis, S.T. (2011). Three theories of privacy: An overview. In S. Trepte & L. Reinecke (Eds.), *Privacy Online* (9-17). Springer.
- Martin, K.D., Borah, A., & Palmatier R.W. (2017) Data privacy: effects on customer and firm performance. *Journal of Marketing*, 2017(81), 36-68.
- Martin, K.D., Kim, J.J., Palmatier, R.W., Steinhoff, L., Stewart, D.W., Walker, B.A., Wang, Y., & Weaven, S.K. (2020). Data privacy in retail. *Journal of Retailing*, 96(4), 474-489.
- Martin, K. (2020). Breaking the privacy paradox: The value of privacy and associated duty of firms. *Business Ethics Quarterly*, 30(1), 65-96.
- Martin, K. D., & Palmatier, R. W. (2020). Data Privacy in Retail: Navigating Tensions and Directing Future Research. *Journal of Retailing* 96(4), 449-457.
- Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50(4), 370-396.
- Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review*, 93(5), 96-105.
- Okazaki, S., Eisend, M., Plangger, K., Ruyter, K., & Grewal, D. (2020). Understanding the strategic consequences of customer privacy concerns: a meta-analytic review. *Journal of Retailing* 96(4), 458-473.
- Palmatier, R. W., & Martin, K. D. (Eds.). (2019). *The intelligent marketer's guide to data privacy: The impact of big data on customer trust*. Springer Nature Switzerland AG.
- Peter, J., & Valkenburg, P.M. (2011). Adolescents' online privacy: Toward a developmental perspective. In S. Trepte & L. Reinecke (Eds.), *Privacy Online* (221-234). Springer.
- Saeri, A. K., Ogilvie, C., La Macchia, S.T., Smith, J.R., & Louis, W.R., (2014). Predicting Facebook users' online privacy protection: Risk, trust, norm focus theory, and the theory of planned behavior. *Journal of Social Psychology*, 154(4), 352-369.
- Schwartz, B. (1968). The social psychology of privacy. *The American Journal of Sociology*, 73(6), 741-752.
- Schwartz, K. M. (2019). The personalization-privacy paradox explored through a privacy calculus model and Hofstede's model of cultural dimensions. Unpublished honor's project. Seattle Pacific University.
- Smith, B., & Browne, C. A. (2021). *Tools and weapons: The promise and the peril of the digital age*. Penguin.
- Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *Management Information Systems Quarterly*, 989-1015.
- Stuart, A., Bandara, A. K., & Levine, M. (2019). The psychology of privacy in the digital age. *Social & Personality Psychology Compass*, 13(11), 1-14.
- Westin, A. F. (1967). Special report: legal safeguards to insure privacy in a computer society. *Communications of the ACM*, 10(9), 533-537.
- Wolfe, M., & Laufer, R. S. (1974). The concept of privacy in childhood and adolescence. In D.H. Carson (Ed.), *Man-environment interactions Part 2, Vol 6*, Washington DC, Environmental Design Research Association.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile books.

# From privacy vulnerability to privacy resilience

At Microsoft, we value, protect, and defend privacy. We believe in transparency, so that people and organizations can control their data and have meaningful choices in how it is used. We empower and defend the privacy choices of every person who uses our products and services.

We ground our privacy commitments in strong data governance practices, so you can trust that we'll protect the privacy and confidentiality of your data and will only use it in a way that's consistent with the reasons you provided it.

To learn more about safeguarding personal data and building a privacy-resilient workplace check out [Microsoft Privacy](#)

» Learn more here:

[Privacy – Microsoft privacy](#)

