Feeling Insecure

CONSUMER WORRIES ON DATA SECURITY AND PRIVACY

KEY POINTS:

- Consumers' concern over their data privacy has increased, and they have relatively little faith in how companies or other entities manage their data.
- However, consumers continue to share their personal information, recognizing it as the price of entry for interacting in a digital world.
- As companies consider data security and privacy measures, legislation is slowly being introduced to improve consumer protections.
- Companies that are proactive, transparent, and receptive to feedback on data security and privacy can gain consumer trust and strengthen their brands.

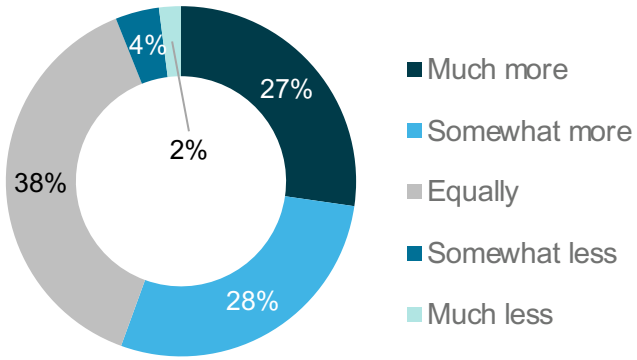
CONCERNS OVER DATA PRIVACY HAVE INCREASED

Consumers are increasingly worried about the security of their personal information, and their increased reliance on technology over the last few years—especially during the pandemic—has only exacerbated this concern. Findings from Burke's Omnibus Tracking Program in November 2021 show that over half of consumers say they're more concerned about their data security than they were one year ago.[1]

As we see, 55% of U.S. consumers are at least somewhat more worried about their data security and privacy compared to the previous year, and an additional 38% are as worried. Worry is higher among older (65+), Black/African American, and middle-income ($50-75K per year) consumers.

OVER HALF OF CONSUMERS ARE MORE CONCERNED ABOUT DATA SECURITY AND PRIVACY COMPARED TO THE PREVIOUS YEAR

Level of concern about data security and privacy relative to the previous year[1]

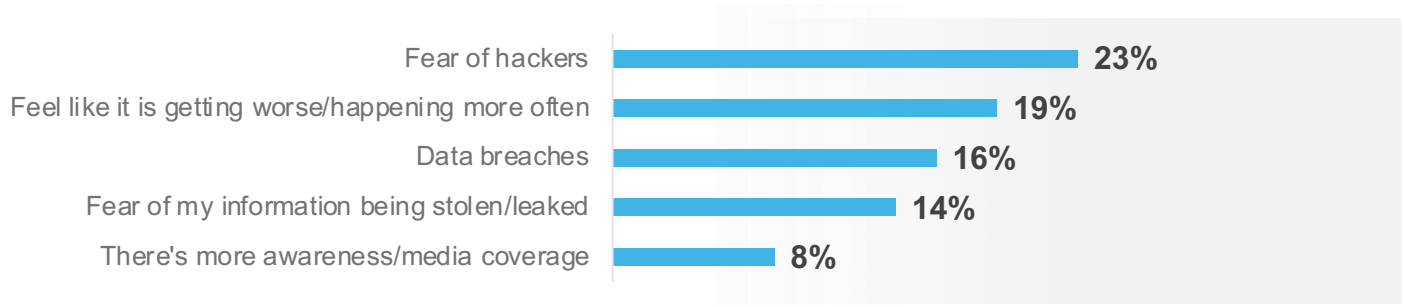


[1]*Burke Omnibus Tracking Program. (November, 2021). November 2021 Data Security and Consumer Concerns*.

Given the rise in data breaches in the past few years, even before the potential for increased cybersecurity threats from Russia due to the invasion of Ukraine, consumers are not wrong in worrying about the security of their personal information. According to the Identity Theft Resource Center, data breaches increased 68% between 2020 and 2021 to the highest total on record.[2] Recent high-profile cyberattacks, such as those on RobinHood, Colonial Pipeline, Microsoft, and T-Mobile, further rattled consumers' faith that corporations are able to keep their information secure. Indeed, Burke's Omnibus results show that one of the top fears consumers have about data security and privacy is that it's getting worse.[3]

WHILE HACKERS REMAINS THE TOP FEAR, CONSUMERS ALSO FEEL DATA BREACHES NOW HAPPEN MORE OFTEN, RAISING ANXIETIES

Top reasons for being concerned about data security and privacy among those somewhat/much more concerned compared to last year[3]

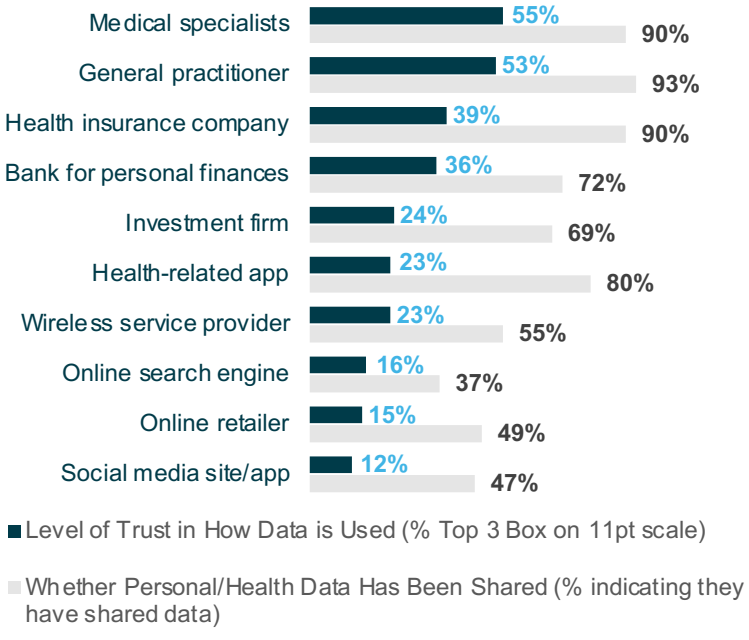


CONSUMERS ARE WARY OF HOW COMPANIES USE DATA, BUT THEY STILL SHARE IT

Concerns about consumers' personal information does not come solely from data breaches and malicious hackers. Consumers are increasingly wary of how companies use their personal information and do not have confidence that their data will be used and secured appropriately. Burke Omnibus results show that trust is relatively low for most organizations and platforms on data use and security.

Among this list of organizations and platforms that frequently use personal data, only healthcare providers (both general practitioners and specialists) garnered trust from at least half of consumers; other firms, such as health insurance companies and banks, are trusted by only a third of consumers. In contrast to these more established institutions, health apps, wireless providers, online search and retailers, and social media apps are trusted by less than a quarter of consumers.[4]

MANY CONSUMERS SHARE DATA DESPITE LOW TRUST ON HOW DATA IS USED



[2]*Identity Theft Resource Center. (2022, January). 2021 Data Breach Annual Report.*
[3]*Burke Omnibus Tracking Program. (November, 2021). November 2021 Data Security and Consumer Concerns.*
[4]*Ibid*

Yet consumers also recognize that giving away their personal information is essentially required to fully engage with many modern conveniences. Thus, despite their apparent lack of trust, many consumers acknowledge giving their information to these same entities, creating cognitive dissonance that may cause anxiety for consumers.

HEALTH-RELATED APPS ARE POPULAR, BUT CONSUMERS ARE WARY OF THEIR SECURITY

The convenience of digital access to health data appeals to consumers. Research from Pew Research[5] shows that Americans want convenient, but secure, access to health data via apps. Consistent with results from Pew, research from the Burke Omnibus study shows that American consumers are comfortable using apps for healthcare purposes. Over a third of US consumers say they are comfortable using healthcare apps; comfort is similar for apps that ask for general information as well as specific health conditions. Younger consumers (age 18-44) are more comfortable with using health apps than older consumers.[6]

However, consumers may be expecting their healthcare apps to have more security than they do. In the Pew research, when consumers were told that U.S. laws do not currently ensure data security on apps, the incidence of consumer security concern rose from 35% to 62%. While incomplete, some movement has been seen on the legislative front for data breaches in health apps: in September 2021, the Federal Trade Commission clarified the Health Breach Notification Rule to include health apps, stating that breach notification requirements within HIPAA apply to apps. The FTC stated that the collection of "personal health records" by devices makes app developers "health care providers" because they provide health care services or supplies.[7] However, the concern from consumers bolsters the need for companies to move beyond the FTC's recent federal breach notification requirements as they apply to health apps; making data in these apps secure is also necessary.

[5]Pew Research. (2021, July 27). Most Americans Want to Share and Access More Digital Health Data. The Pew Charitable Trusts. Retrieved November 17, 2021, from

https://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2021/07/most-americans-want-to-share-and-access-more-digital-health-data

[6]Burke Omnibus Tracking Program. (November, 2021). November 2021 Data Security and Consumer Concerns.

[7]Federal Trade Commission. (September 15, 2021). Statement of the Commission on Breaches by Health Apps and Other Connected Devices. Retrieved November 17, 2021, from https://www.ftc.gov/public-statements/2021/09/statement-commission-breaches-health-apps-other-connected-devices.

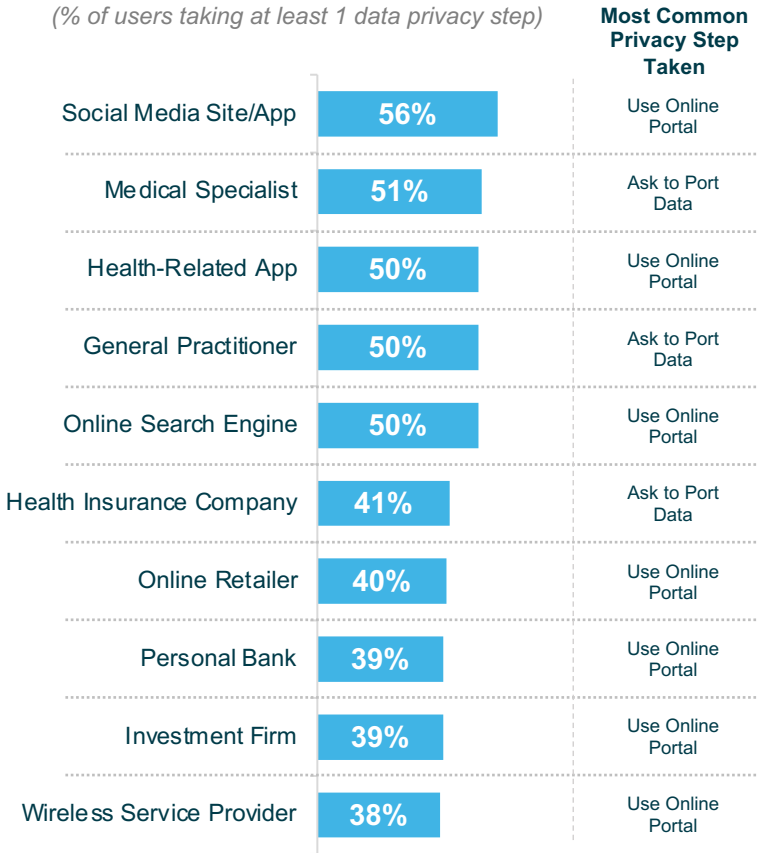
SOME CONSUMERS HAVE CONVERTED THEIR CONCERNS INTO ACTION BY CONTROLLING THE DATA THEY'VE SHARED

Part of the California Consumer Privacy Act (CCPA), effective in January 2020, gives California consumers certain rights regarding the personal data organizations have. For example, consumers can learn what data they have and how they are used, ask to port the data to another entity, use an online portal to select what personal data a company may use, and request that companies anonymize or even delete their personal data. Companies that do business in California are obligated to allow California consumers to request these steps to protect their data, and some companies have proactivity allowed all consumers—regardless of their home state—to take these actions.

Burke's Omnibus Tracking Program[8] sheds light on whether consumers are taking these data control and security steps in US states where laws do not guarantee their rights to do so, i.e., in states other than California. Currently, between a third and a half of US consumers have taken one or more steps to control the data they share, depending on the nature of the platform or business. The type of actions consumers have taken also depends on who has the data: consumers tend to ask those providing health-related services (health insurance, general practitioners, specialists) to port data elsewhere, but for digital platforms (search engines, social media apps, health apps, etc.) they tend to use an online portal to restrict data. As these data control measures become more popular, companies should be ready to accommodate more consumer requests.

HALF OF CONSUMERS HAVE ASKED COMPANIES TO PROTECT THEIR DATA

(% of users taking at least 1 data privacy step)



Data privacy steps include: asking companies what data they store, asking how data are used, asking to port data to another entity, asking to anonymize data, using an online portal to restrict data, and asking to delete data

COMPANIES HAVE ROOM TO IMPROVE ON DATA SECURITY, AND LEGISLATION MAY FORCE THEIR HAND

Unfortunately for consumers, many companies are not on the forefront of data security and privacy. A recent KPMG survey of executives found that 62% of firms say their company should be doing more to strengthen data protection measures, while 70% say they have actually increased the amount of personal data they collect in the past year.[9] Firms clearly want to do right by their consumers, but given the strong business value of consumer data and lack of legislative guardrails, executives may not feel empowered yet to create their own.

However, these legislative guardrails may be coming soon. The introduction of the General Data Protection Regulation (GDPR) in Europe in 2018 has had a substantial impact on privacy laws around the world. In the US, state governments have had some data privacy legislative success, with the CCPA becoming law at the start of 2020. Both Colorado and Virginia's data privacy laws will become effective in 2023, and several other states have bills under consideration.

[8]*Burke Omnibus Tracking Program. (November, 2021). November 2021 Data Security and Consumer Concerns.*
[9]*KPMG. (2021, August). Corporate Data Responsibility: Bridging the Consumer Trust Gap.*

Furthermore, there is strong evidence that consumers want broad data privacy legislation. A recent poll from the Associated Press and NORC Center for Public Affairs Research found that 74% of Americans support establishing national standards for how companies can collect, process, and share personal data, and over 70% want the federal government to treat personal data security as a national security issue.[10]

BEING PROACTIVE ABOUT DATA SECURITY BEFORE LEGISLATION IS ENACTED CAN HELP COMPANIES GAIN CONSUMERS' TRUST

Consumers are clearly anxious about the security and use of their personal information online, and their fears are increasing each year. Given the lack of movement on the legislative front for broad data security policy, this presents companies with a unique opportunity to gain consumer trust, and thus help boost consumer loyalty[11], by being proactive on data security. Steps companies can take include:

CREATE, AND COMMUNICATE, DATA SECURITY MEASURES

The GDPR and other legislation has created a template for what data security measures will entail. Create data security and privacy policies for your consumers and let them know that you are being active in this area.

BE TRANSPARENT

Tell consumers what you use their data for, where it goes, and how it is secured. Consumers are willing to give their information to interact with the digital world, and companies that can help alleviate their anxiety will earn respect and trust.

BE RECEPTIVE TO FEEDBACK

Along with letting consumers know about your use of their data, listen to them about what is and is not acceptable use. Digital privacy is a new arena, and companies that co-create policies and standards alongside their consumers will again gain trust and strengthen their brand.

U.S. consumers are nervous about how their personal information is used and secured online, but feel forced to give this data away in order to engage in the digital world. The anxiety created by this contradiction is an opportunity for companies to create trust with their consumers by being proactive and engaged in improving data privacy. Given the upcoming increase in data privacy legislation, waiting too long to make changes may lead to brands seeming complacent and only changing because they are forced.

ABOUT THE AUTHOR

JEREMY COCHRAN, PSYD
Research & Development Manager

Jeremy is a psychologist, 10-year veteran of the insights industry, and lifelong learner.

CONTACT: JEREMY.COCHRAN@BURKE.COM

[10] MeriTalk & The Associated Press-NORC Center for Public Affairs Research. (2021, September). Trust in Government is Low, But Americans are United Around Investments In Technology.
[11] Bernarto, I., Berlianto, M. P., Palupi, Y. F. C., Meilani, M., Masman, R. R., & Suryawan, I. N. (2020). The influence of brand awareness, brand image, and brand trust on brand loyalty. Jurnal Manajemen.