DATA PRIVACY DAY IS JANUARY 28TH

GET #PRIVACYAWARE IN THE NEW DECADE!

CHAMPIONS BACKGROUNDER

DATA PRIVACY DAY

WHAT IS DATA PRIVACY DAY?

Led by the National Cyber Security Alliance (NCSA), Data Privacy Day began in the United States and Canada in January 2008 as an extension of Data Protection Day in Europe. Observed annually on January 28, Data Protection Day commemorates the January 28, 1981 signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection.

Each year, data breaches continue to grow in size and scope – exposing consumers' sensitive, personal information and businesses' valuable data. Against this backdrop, Data Privacy Day helps spread awareness about privacy and educates citizens on how to secure their personal information. It also works to encourage businesses to be more transparent about how they collect, store and use data.

To promote these goals, Data Privacy Day's 2020 theme is "Own Your Privacy."

> ***"With the California Consumer Privacy Act going into effect in January 2020, this year's Data Privacy Day couldn't be more timely for increasing awareness among businesses and consumers about the importance of respecting and protecting personal information," said Kelvin Coleman, executive director of NCSA. "With the tremendous growth of businesses collecting and using personal data and millions of customers putting private information online, Data Privacy Day works to encourage businesses to improve data privacy and security practices and educate consumers about the many ways their personal information can be used and shared."***

MEDIA CONTACT: Jessica Beffa
+1 720-413-4938 | NCSA@thatcherandco.com

WHY WE SHOULD CARE ABOUT ONLINE PRIVACY

With the California Consumer Privacy Act taking effect this year and other states considering similar legislation, data privacy will become a central issue for businesses in 2020. Yet while consumers conduct much of their lives on the internet via connected devices, few understand the critical issue of privacy and how their personal information is used, collected and shared by businesses. This data can be stored indefinitely and used in both beneficial and unwelcome ways. Even seemingly innocuous information – such as your favorite restaurants or items you purchase – can be used to make inferences about your socioeconomic status, preferences and more.

Many companies have the opportunity to monitor their users' and customers' personal behavior and sell the data for profit. In order to make informed decisions and understand the true value of their data, consumers need to understand how it is collected, used and shared.

WHAT IS THE DIFFERENCE BETWEEN PRIVACY AND SECURITY?

Security refers to the ways we protect ourselves, our property and personal information. It is the first level of defense against unwanted intruders. Privacy is our ability to control access to our personal information.

MEDIA CONTACT: Jessica Beffa
+1 720-413-4938 | NCSA@thatcherandco.com

PRIVACY TIPS FROM NCSA

ADVICE FOR CONSUMERS: SAFEGUARDING YOUR DATA

Your mobile devices – including smartphones, laptops and wearables – are always in reach wherever you go, and they share substantial information about you and your habits. Follow these basic privacy tips to help you better manage your personal information.

TIPS TO HELP PROTECT YOUR PRIVACY

- **Personal info is like money: Value it. Protect it.** Information about you, such as your purchase history or location, has value – just like money. Be thoughtful about who gets that information and how it's collected through apps and websites. You should delete unused apps, keep others current and review app permissions.
- **Share with care.** Think before posting about yourself and others online. Consider what it reveals, who might see it and how it could be perceived now and in the future.
- **Own your online presence.** Set the privacy and security settings on websites and apps to your comfort level for information sharing. Each device, application or browser you use will have different features to limit how and with whom you share information.
- **Think before you act.** Information about you, such as the games you like to play, your contacts list, where you shop and your geographic location, has tremendous value. Be thoughtful about who gets that information and understand how it's collected through websites and apps.

ADVICE FOR ORGANIZATIONS: PRIVACY IS GOOD FOR BUSINESS

Protecting your customers' privacy is a competitive advantage. Respecting consumers' privacy is a smart strategy for inspiring trust and enhancing reputation and growth.

Tips for Transparency and Trust

- **Privacy is everyone's business: If you collect it, protect it.** Follow reasonable security measures to keep individuals' personal information safe from inappropriate and unauthorized access.
- **Transparency builds trust.** Be open and honest about how you collect, use and share consumers' personal information. Think about how the consumer may expect their data to be used and design settings to protect their information by default.
- **Build trust by doing what you say you will do.** Communicate clearly and concisely to the public what privacy means to your organization and the steps you take to achieve and maintain privacy.
- **Conduct due diligence and maintain oversight of partners and vendors.** If someone provides services on your behalf, you are also responsible for how they collect and use your consumers' personal information.

MEDIA CONTACT: Jessica Beffa
+1 720-413-4938 | NCSA@thatcherandco.com

FIVE WAYS TO HELP EMPLOYEES BE #PRIVACYAWARE

Educate employees on the importance and impact of both protecting consumer and colleagues' information and the role they play in keeping it safe.

- **Help employees manage their individual privacy.** Encourage employees to update their individual account privacy settings by visiting Update Your Privacy Settings on staysafeonline.org
- **Host a "lunch and learn."** Invite experts to talk to employees about why privacy matters. Engage staff by asking them to consider how privacy and data security applies to the work they do on a daily basis, regardless of the department. You could even invite your employees to join NCSA's Data Privacy Day event virtually via livestream on Jan. 28.
- **Create a #PrivacyAware culture.** Encourage all employees to sign up as Data Privacy Day Champions! It's free and NCSA will provide a toolkit with valuable, user-friendly resources. Share messages about privacy throughout the office, on internal message boards or through available communication platforms now through Jan. 28.
- **Give Back.** Talk to young people about why privacy matters. Organize a company-wide volunteer day with local schools to teach students about privacy and online safety. Use these easy-to-follow tips to help you get started.
- **Have fun while learning.** Organize a scavenger hunt, competition or game that helps employees learn about the importance of privacy. Recognize and reward employees for being #PrivacyAware.

MEDIA CONTACT: Jessica Beffa
+1 720-413-4938 | NCSA@thatcherandco.com

STORY IDEAS

Privacy affects every part of our life both at home and at work. To help encourage #PrivacyAware habits at home and on the job, NCSA has compiled a wide range of story ideas about everyday privacy concerns and challenges.

PARENTING

- Are You Oversharenting? How to Manage Your Family's Online Exposure
- How to Teach Your Teens About Privacy
- Five Ways Your Child's Data is Being Exposed

EDUCATION

- Is Your School District Protecting Your Child's Privacy?
- Connected Classrooms and Privacy Concerns

ALL ABOUT APPS

- How to Understand an App's Privacy Policy
- Location Tracking Apps: 3 Privacy Settings You Need to Know
- How Your Apps are Collecting Your Data and What They're Doing with It

HEALTHCARE

- Is Your Doctor Practicing Good Data Hygiene?
- Why You Should Care About Your Healthcare Data

GENERAL

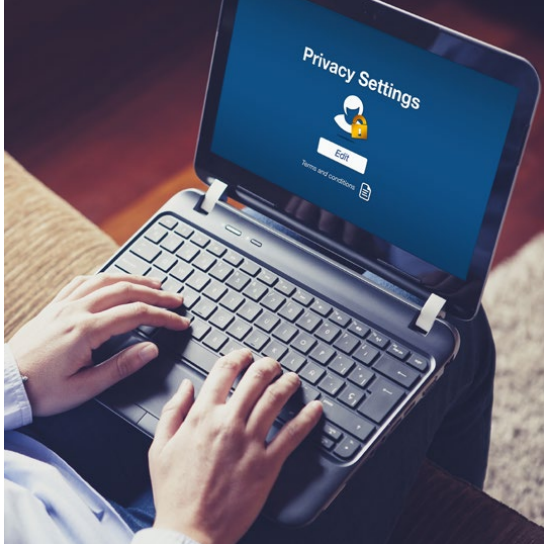
- Is Your Favorite Company Spying on You?
- What Your Voice Assistant Knows About You
- How to Opt Out of a Company's Data Sharing Practices
- The Right to Be Forgotten

MANAGING YOUR SOCIAL MEDIA LIFE

- Three Questions to Ask Yourself Before Posting a Picture to Social Media
- Just Some Social Media Fun? Think Again! The Privacy Dangers of Popular Quizzes and Games
- How to Research Your Online Reputation

ENTERPRISE AND SMALL BUSINESS

- What Do You Need to Know About GDPR or the new California Consumer Privacy Act
- Why Data Privacy is Good for Business
- Artificial Intelligence, Machine Learning and Privacy: What Your Business Should Know
- How to Create a Culture of Privacy in the Workplace



FAST FACTS AND STATS

CONSUMERS ARE CONCERNED ABOUT PRIVACY

As the issue of privacy becomes more familiar to the public, consumers are becoming more concerned about who can access their information and why. A recent survey by Pew Research Center found that majorities of Americans think their personal data is less secure now than five years ago and that data collection poses more risks than benefits. For example:

- A majority of Americans report being concerned about the way their data is being used by companies (79 percent) or the government (64 percent).
- Fully 79 percent of Americans say they are not too confident or not at all confident that companies will admit mistakes and take responsibility if they misuse or compromise personal information, and 69 percent report having this same lack of confidence that firms will use their personal information in ways they will be comfortable with.
- Many Americans acknowledge that they are not always diligent about paying attention to privacy policies and terms of service.
  - Only about 1 in 5 adults say they always (9 percent) or often (13 percent) read privacy policies.
- 78 percent of adults in the United States say they understand very little or nothing about what the government does with the data it collects.
  - 59 percent say the same about the data companies collect.
  - 63 percent say they have very little or no understanding of the laws and regulations that are currently in place to protect their privacy.

PROTECTING THE CONNECTED HOME

Most households now run networks of devices linked to the internet including computers, gaming systems, household assistants, home robots, TVs, tablets, smartphones and wearables. These devices make it easier to connect to the world around you, but they can also track your personal information, including your contacts, photos, videos, location and health and financial data.

- Approximately 29 billion connected devices are forecasted to be in use by 2022, of which around 18 billion will be related to IoT.[1]
- 36 percent of people in the United States own six web-connected devices or more[2], and 90 percent of Americans own a smart home device.[3]
- One-quarter of adults in the United States say they have a smart speaker in their home.[4]
- The use of connected, smart home devices is expected to increase from 33.2 percent in 2019 to 53.9 percent by 2023.[5]
- The number of smart homes in the United States is expected to hit 28 percent of total households by 2021.[6]
- While 85 percent of enterprises are in the process of or intend to deploy IoT devices, only 10 percent feel confident that they could secure those devices against security threats, according to AT&T's Cybersecurity Insights Report.[7]
- Recent events also have changed the way manufacturers think about collecting data. In Jabil's 2018 Connected Home and Building Technology Trends Survey, 69 percent of solution providers surveyed noted that the recent focus on data privacy, including the scandal at Cambridge Analytica, has made them rethink their plans to collect and use data from smart devices.[8]

PRIVACY, PARENTING AND TEENS: INSIGHTS FROM THE NCSA/MICROSOFT "KEEPING UP WITH GENERATION APP" SURVEY

In this digitally-connected age, teens and parents continue to spend a lot of time online despite their concerns about security and privacy. Highlights from a recent parent-teen NCSA/Microsoft survey include:[9]

- 39 percent of teens said they were concerned about their personal information being leaked online and 36 percent had this same worry as it pertains to pictures and videos that are shared privately.
- Teens and parents are closely aligned on their top three concerns affecting online teens (ranked as something they are "very concerned" about), which are:
  - Someone accessing a teen's account without permission (teens 41 percent vs. parents 41 percent).
  - Someone sharing a teen's personal information about them online (teens 39 percent vs. parents 42 percent).
  - Having a teen's photo or video shared that they wanted private (teens 36 percent vs. parents 34 percent).
- 57 percent of teens say they have created an account that their parents are unaware of, such as a social media site or an app they wanted to use.

1. https://www.ericsson.com/en/mobility-report/internet-of-things-forecast
2. https://www.pymnts.com/news/payment-methods/2018/consumer-trends-mobile-voice-biometrics-cash/
3. https://www.iottechnews.com/news/2018/may/15/research-us-consumers-smart-home-device/
4. https://www.pewresearch.org/fact-tank/2019/11/21/5-things-to-know-about-americans-and-their-smart-speakers/
5. https://www.safesmartliving.com/smart-home/statistics-and-predictions/
6. https://www.spglobal.com/marketintelligence/en/news-insights/blog/smart-homes-in-the-u-s-becoming-more-common-but-still-face-challenges
7. https://www.businessinsider.com/internet-of-things-security-privacy-2016-8
8. https://www.iotforall.com/smart-home-data-security/
9. https://staysafeonline.org/resource/keeping-generation-app-2017/

SOCIAL MEDIA

Social media is a great platform for connecting with friends and family through personal news updates, photo sharing and live streaming. As convenient and fun as these platforms are, privacy settings don't always prevent personal information from being shared beyond the intended audience and without a user's knowledge.

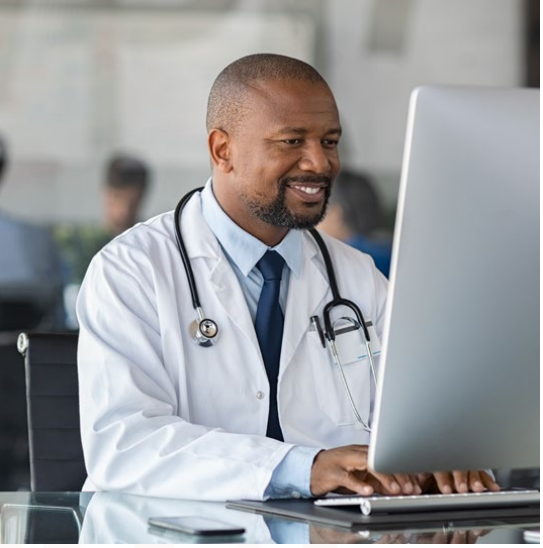
- 61 percent of people think social media companies do not adequately protect consumer data.[10]
- 82 percent of cyber stalkers use social media to find out information about potential victims – for example, where they live and which school they attend.[11]
- The NCSA/Microsoft 2017 "Keeping up with Generation App" survey revealed that across the board from a privacy perspective, teens report that they are "very concerned" about someone:
  - Accessing their accounts without their permission (41 percent)
  - Sharing personal information about them online that they prefer to keep private (39 percent)
  - Posting a private photo or video of them online (36 percent)

RETAIL AND YOUR DATA

E-commerce is a thriving industry that provides a great convenience for consumers. It is, however, an environment ripe for cybercrime with millions of consumers' banking information, addresses and browsing preferences and data potentially available. Online shoppers must be careful by protecting their personal data and ensure they are doing business over secure networks.

- A majority of consumers are willing to walk away from a business entirely if it suffers a data breach, with retailers most at risk: 62 percent of people said they would no longer do business with a retailer that had experienced a data breach compared to 59 percent who said the same for banks and 58 percent who said so about social media sites.[12]
- More than 70 percent of consumers are unaware of tools they can use to control or limit the usage of their personal data.[13]
- Nearly one-third of consumers do not know that many of the "free" online services they use are paid for via targeted advertising made possible by the tracking and collecting of their personal data.[14]
- Close to 77 percent would like more transparency on the ads being targeted to them based on the personal data the internet companies collect.[15]
- An AARP Cyber Security survey found that about four out of 10 consumers use free Wi-Fi at least once a month, and among those, one-third had made a purchase on free Wi-Fi with a credit card in the last six months.[16]

10. https://www.apnews.com/c9c1aa5d1c4546db91d85be1fe9fbca9
11. http://socialbarrel.com/social-media-privacy-infographic/101217/
12. https://www.apnews.com/c9c1aa5d1c4546db91d85be1fe9fbca9
13. http://www.telecompetitor.com/being-the-product-for-internet-giants-raises-privacy-concerns-for-consumers/
14. http://www.telecompetitor.com/being-the-product-for-internet-giants-raises-privacy-concerns-for-consumers/
15. http://www.telecompetitor.com/being-the-product-for-internet-giants-raises-privacy-concerns-for-consumers/
16. https://www.aarp.org/money/scams-fraud/info-2016/dangers-of-free-public-wifi-ea.html



HEALTHCARE AND DIGITAL RECORD KEEPING

Technology can greatly improve the delivery of medical and health services for patients. As healthcare companies turn to digital record keeping and internet-connected medical devices, patient outcomes are also improving. But these advances in healthcare technology also come with a risk: medical organizations, including insurance companies, collect large volumes of data that we report on our devices, including our Social Security numbers, financial information, medical history and current health status. This data can be immensely valuable to cybercriminals and so intensely personal that patients would be deeply impacted if it was lost or stolen. Recent statistics found that:

- In healthcare, the average cost of a breach has increased to $429 per record from $408 last year – an increase of 5.15 percent. In the United States, the average healthcare data breach costs $15 million.[17]
- Globally, the healthcare industry has the highest breach costs with an average mitigation cost of $6.45 million; these breaches typically cost 65 percent more than data breaches experienced in other industry sectors.[17]
- Four in five physicians in the United States have had cyberattacks in their practices, according to an Accenture survey.[18]
- About 78 percent of respondents to a recent survey of healthcare professionals said they'd had experienced either a malware and/or ransomware attack in the last 12 months.[19]
- Under the Health Insurance Portability and Accountability Act (HIPAA), it's illegal for healthcare providers to share patients' treatment information. More than 30,000 reports regarding privacy violations are received each year.[20]

17. https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/
18. https://newsroom.accenture.com/news/four-in-five-us-physicians-have-had-a-cyberattack-in-their-clinical-practices-says-survey-by-accenture-and-the-american-medical-association.htm
19. https://healthitsecurity.com/news/78-of-providers-report-healthcare-ransomware-malware-attacks
20. http://www.npr.org/sections/health-shots/2015/12/10/459091273/small-violations-of-medical-privacy-can-hurt-patients-and-corrode-trust

PRIVACY IS GOOD FOR BUSINESS

General Data Protection Regulation (GDPR) and the California Consumer Privacy Act, among others, have made privacy a top priority for businesses in 2018 and 2019. Against this backdrop, Cisco's 2018 Privacy Maturity Benchmark Study showcased the importance of having good privacy processes well beyond GDPR compliance and also highlighted some of the financial benefits.[21] Some of the top findings from the study include:

- Sales delays due to data privacy concerns are widespread and significant in length. 65 percent of organizations reported that they have delays in their sales cycle, and among all respondents, the average sales delay was 7.8 weeks.
- The sales delays varied by country and industry. The longest delays by country occurred in Latin America and Mexico, and by industry in the government and healthcare sectors. Notably, the average sales delay was highly correlated with the privacy maturity level of the organization.
- Sales delays also varied significantly by the organizational model adopted for the privacy resources. A hybrid model, which has a mix of centralized and decentralized privacy resources, had shorter delays (4.6 weeks), compared to models with fully centralized (9.8 weeks) or decentralized resources (7.1 weeks).
- The level of privacy maturity also correlated with the likelihood and costs of data breaches. 74 percent of privacy-immature companies experienced a cyber loss of over $500,000 in the last year, compared to only 39 percent of privacy-mature companies.

21. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/privacy-maturity-benchmark-study.pdf

LIVE FROM LINKEDIN

JOIN US FOR DATA PRIVACY DAY 2020

Recent years have been transformational for privacy. In the wake of GDPR, governments around the country and around the world, are enacting privacy laws and regulations. Data Privacy Day 2020 will bring together experts on United States and international privacy to delve deep into the global wave of regulations and what they mean for economies around the world today and into the future.

Data Privacy Day 2020 will convene data privacy experts from industry, government, academia and non-profit for a morning of TED-style talks, panels and chats on global data privacy regulations.

WHEN

TUESDAY, JAN. 28, 2020
FROM 8:30AM – 12:30 P.M PST

WHERE

LINKEDIN, 222 2ND STREET,
SAN FRANCISCO, CA

CONTRIBUTING SPONSORS

VISA
Microsoft
INTEGRIS SOFTWARE

GLOBAL SPONSORS

TREND MICRO
The experts in screen privacy. | 3M
KnowBe4 Human error. Conquered.
yubico

EVENT PARTNER

ITSP MAGAZINE

AGENDA OVERVIEW (ALL TIMES PST)

8:30 a.m. – 10:00 a.m.	**Media Briefing**
10:00 a.m. – 10:05 a.m.	**Opening Remarks**
10:05 p.m. – 12:20 p.m.	**Executive Panel & Talks**
12:20 p.m. – 12:25 p.m.	**Closing Remarks**

EXECUTIVE PANELS INCLUDE:

+ **International Perspectives: Privacy Across the Globe:** How has GDPR changed the privacy landscape across the globe? Experts will come together to discuss the recent European legislation and the privacy approaches of countries around the world.
+ **Panel: U.S. Government Perspectives - CCPA and the Wake of Privacy Legislation in the U.S.:** The California Consumer Privacy Act is the first legislation of its kind within the United States. Experts will discuss the impact of CCPA, how other states are creating or enforcing privacy legislation and how these separate laws affect our nation's privacy as a whole.
+ **Industry Perspectives: Going Beyond Privacy Compliance:** Industry leaders and influences will address in detail how to not only comply with current regulations but how to prepare for future laws and make protecting customers' data a top priority.

The latest agenda as well as livestream details for the executive sessions are available here.

If you are interested in attending this event as a member of the media, please email Thatcher+Co. at ncsa@thatcherandco.com.

To see a list of other NCSAM events around the country, including virtual events, click here.

GET INVOLVED

BECOME A DATA PRIVACY DAY CHAMPION

I AM #PRIVACYAWARE

Americans everywhere can join the #PrivacyAware campaign – it's easy to do and will help generate awareness about the importance of data privacy. Empower others to protect their personal online data by tweeting, "I am #PrivacyAware, are you? Find out at https://staysafeonline.org/data-privacy-day/."

Organizations and individuals who want to officially show support for Data Privacy Day can become a Data Privacy Day Champion. Champions represent those dedicated to respecting privacy, safeguarding data and enabling trust. Being a Champion is easy and does not require any financial support. Champions receive a toolkit of privacy awareness materials that they can use to educate themselves and their communities. Champions can include individuals, companies and organizations of all sizes; schools and school districts; colleges and universities; nonprofits; and government organizations. For more information on how to become a Data Privacy Day 2020 Champion, click here.

IN YOUR COMMUNITY: Privacy experts can get involved by volunteering to share their privacy knowledge in a local school, senior care facility or faith-based organization. Use free resources at staysafeonline.org to spread the word.

GET INVOLVED INFOGRAPHIC: Learn simple, actionable advice you can use to educate people about privacy at home, at work and in your community. Get Involved Infographic

CHECK YOUR PRIVACY SETTINGS: Want to view or change your privacy/security settings, but don't know where to find them? NCSA has an easy-to-use resource with direct links to update your privacy settings on popular devices and online services. Manage Your Privacy Settings

With technology constantly changing, it can be challenging to keep up - and to manage your family's technology usage. That's why Verizon has partnered with leading online safety partners to provide you with resources so you and your family have the confidence to use technology safely and responsibly. Learn more here.

ABOUT US

ABOUT THE NATIONAL CYBER SECURITY ALLIANCE

NCSA is the nation's leading nonprofit, public-private partnership promoting cybersecurity and privacy education and awareness. NCSA works with a broad array of stakeholders in government, industry and civil society. NCSA's primary partners are the Cybersecurity and Infrastructure Security Agency and NCSA's Board of Directors, which includes representatives from ADP; American Express; Bank of America; Cofense; Comcast Corporation; Eli Lilly and Company; ESET North America; Facebook; Google; Intel Corporation; Lenovo; LogMeIn, Inc., Marriott International; Mastercard; Microsoft Corporation; Mimecast; NortonLifeLock; Proofpoint; Raytheon; Trend Micro, Inc.; Uber; U.S. Bank; Visa and Wells Fargo.

NCSA's core efforts include National Cyber Security Awareness Month (October); Data Privacy Day (Jan. 28); and CyberSecure My Business™. For more information on NCSA, please visit staysafeonline.org/about-us/overview/.

ABOUT DATA PRIVACY DAY

The National Cyber Security Alliance's (NCSA) privacy awareness campaign is an integral component of STOP. THINK. CONNECT.™ — the global online safety, security and privacy campaign. Data Privacy Day began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe and is officially led by NCSA in North America. VISA, Microsoft and Integris are "Contributing Sponsors" of the 2020 privacy awareness campaign. TrendMicro, 3M, Knowbe4 and Yubico, are "Global Sponsors." ITSP Magazine is an "Event Partner." The hashtag for NCSA's privacy campaign efforts is #PrivacyAware.

MEDIA ROOM AND PRESS RESOURCES:

https://www.staysafeonline.org/about-us/news/media-room/