2018 EYE ON PRIVACY REPORT

WHAT DOES THE U.S. GENERAL PUBLIC KNOW ABOUT DATA PRIVACY BEST PRACTICES AND REGULATIONS?

MediaPRO
Cybersecurity & Privacy Education

INTRODUCTION

The world as we know it cannot run without the transfer of personal data, all of which needs to be kept secure. Limits on this data transfer can be put in place, user consent requested, and precautions taken, but no shared personal information is ever 100%, unequivocally safe at any given time.

Near-weekly headlines describing the latest breach of personal information by one company or another show how frequently personal data such as birth dates, addresses, and social security numbers are collected, used, and sometimes abused. Even with this much data coursing through cyberspace, many industries and organizations still rely on hard copies of information to manage and retain private data.

No matter the type, all personal data has one thing in common: a real, live human will be responsible for its safekeeping at some point. Just think of the armies of clerks, bank tellers, IT staff, HR workers, etc., who handle personal information as part of their job. Even if personal information never leaves a secure server in some distant warehouse, humans are responsible for keeping out those who would exploit it.

With this much personal data at the hands of everyday people, we wanted to know: what does the general public know about data privacy?

ABOUT THE SURVEY

To attempt to find out, we surveyed 1,007 U.S. residents concerning data privacy best practices and regulations, both national and global, and analyzed the data by age group and industry sector. Every respondent had to be 18 years or older and employed. We asked respondents what they would do in five real-life scenarios that could play out in nearly any corporate office across the country. Each scenario dealt with a different aspect of data privacy knowledge or a privacy best practice. The survey was conducted in October 2017.

HIGH-LEVEL FINDINGS

We go into detail later in the report about the findings in each of the five sections, but here are key takeaways from each section:

SECTION 1: IDENTIFYING SENSITIVE AND PRIVATE DOCUMENTS

Survey respondents were generally good at recognizing a variety of different types of potentially private information, knowing to either destroy it or store it securely as appropriate.

SECTION 2: GRANTING ACCESS TO THIRD-PARTY APPLICATIONS

Respondents 55 years of age and older were more likely than their younger counterparts to never grant any third-party mobile device applications a variety of common permissions.

SECTION 3: DETERMINING THE SENSITIVITY OF SPECIFIC TYPES OF INFORMATION

Finance sector employees did not consider tax information any more sensitive than respondents from the six other industries we included in the survey.

SECTION 4: KNOWLEDGE OF NATIONAL AND GLOBAL PRIVACY REGULATIONS

Respondents across all industries and age groups showed the deepest lack of familiarity with the EU GDPR regulations and the EU-U.S. Privacy Shield framework.

SECTION 5: REPORTING POTENTIAL PRIVACY INCIDENTS

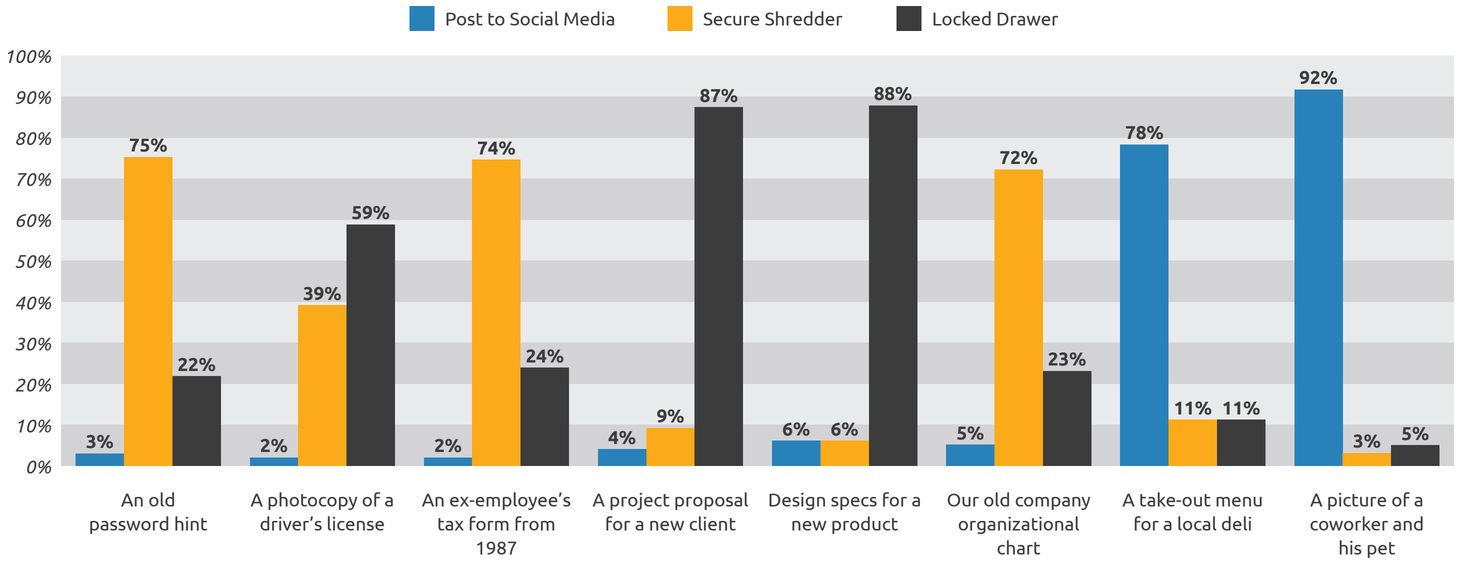
Respondents in the technology sector demonstrated the least ability to correctly identify scenarios that could put private data at risk as reportable privacy incidents.

SECTION 1:
IDENTIFYING SENSITIVE AND PRIVATE DOCUMENTS

We asked respondents to take one of three actions (post to social media, destroy in a secure shredder, or secure in a locked drawer) when presented with the following examples of documents and information commonly found in an office environment:

- An old password hint
- A photocopy of a driver's license
- An ex-employee's tax form from 1987
- A project proposal for a new client
- Design specifications for a new product
- An old company organizational chart
- A take-out menu for a local deli
- A picture of a coworker and his pet

FIGURE 1.1:
CLASSIFYING DOCUMENTS AND POTENTIALLY SENSITIVE INFORMATION



Survey respondents were generally knowledgeable about what types of information deserved secure handling. For example, 87% of respondents chose to correctly store a project proposal for a new client and design specifications for a new product in a locked drawer.

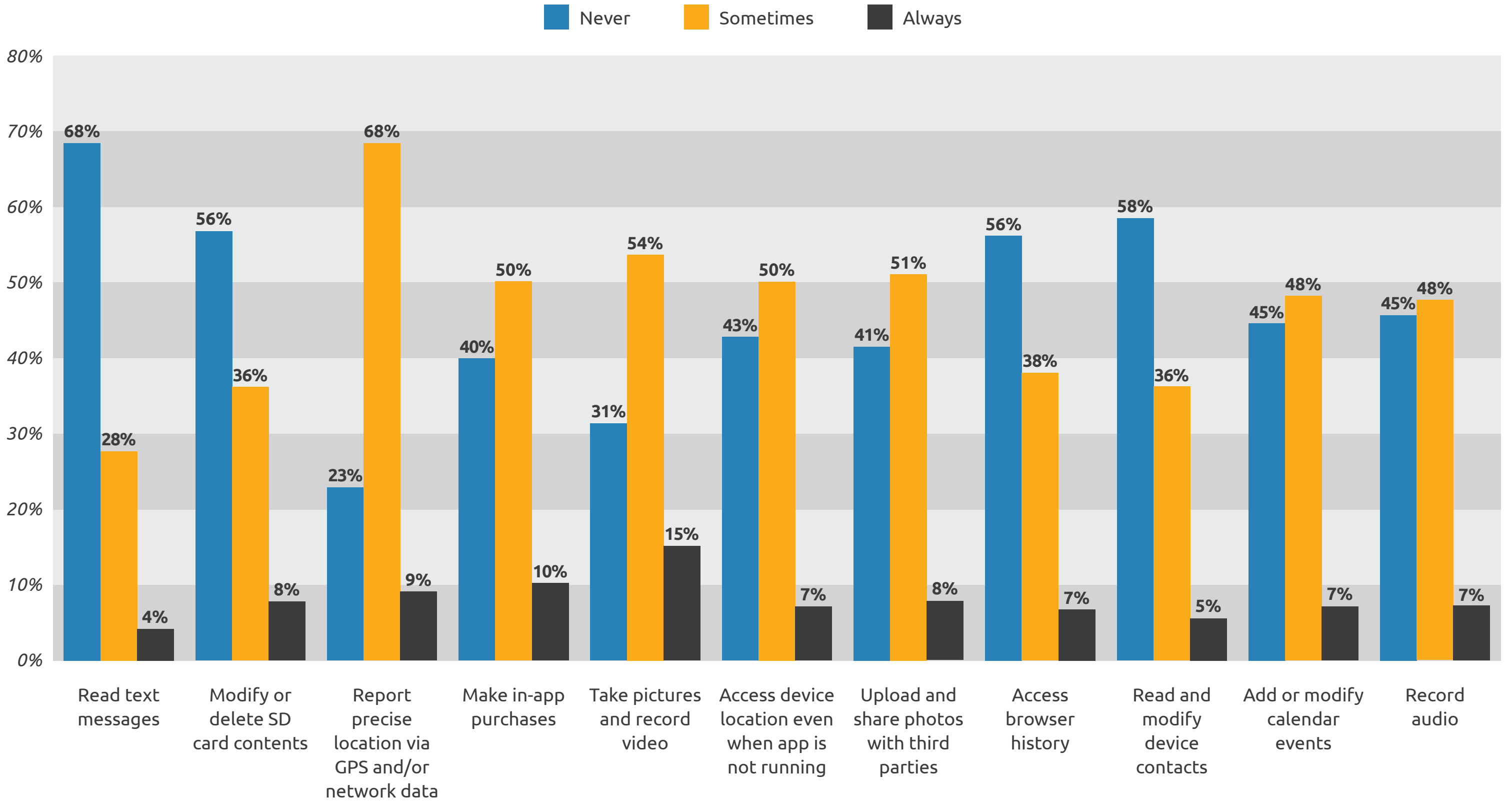
Almost all respondents chose to either destroy an old password hint and an ex-employee tax form from three decades ago in a secure shredder (75% and 74%, respectively) or keep these items in a locked drawer (22% and 24%, respectively). While not the ideal answer for these two pieces of information, the choice to secure them in a locked drawer still showed respondents' understanding that the information in question was sensitive and not for public consumption.

SECTION 2:
GRANTING ACCESS TO THIRD-PARTY APPLICATIONS

Survey respondents were asked how often (either "never," "sometimes," or "always") they granted third-party applications the following permissions on their mobile device:

- Read text messages
- Modify or delete SD card contents
- Report precise location via GPS and/or network data
- Make in-app purchases
- Take pictures and record video
- Upload and share photos with third parties
- Access device location even when app is not running
- Access browser history
- Read and modify device contacts
- Add or modify calendar events
- Record audio

FIGURE 2.1:
HOW OFTEN DO YOU GRANT THE FOLLOWING PERMISSIONS TO THIRD-PARTY APPLICATIONS?

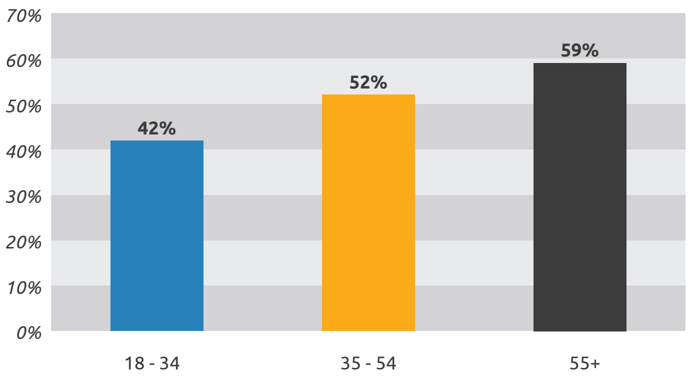


Overall, survey results were mostly mixed between whether respondents “never” or “sometimes” granted third-party applications of the 11 common permissions listed above. Of the 11, the highest percentage (68%) of survey respondents said they never allow a third-party app to access their text messages, suggesting a high value placed on information shared this way. Respondents seemed most comfortable with third-party apps being able to take pictures and video, with 15% saying they’d “always” grant this permission when asked, the highest response for the 11 types of permission asked about.

Interestingly, respondents were more likely to report that they sometimes or always allow apps to access their devices’ precise location (GPS), make in-app purchases, take pictures and video, and upload photos to third-party sites than permission to modify or delete contents of their device’s memory.

Just more than half of respondents (56%) reported that they never allow third-party apps to modify or delete their devices’ memory content, with 36% saying they sometimes do. This suggests at least some misunderstanding about what permissions apps truly have and are granted, as many apps require permission to modify a device’s memory simply to function. A Pew Research Center study from 2015, for example, found that 54% of the apps in the Google Play app store required this permission.

FIGURE 2.2: HOW OFTEN EACH AGE GROUP ANSWERED “NEVER” TO AN APP PERMISSION REQUEST



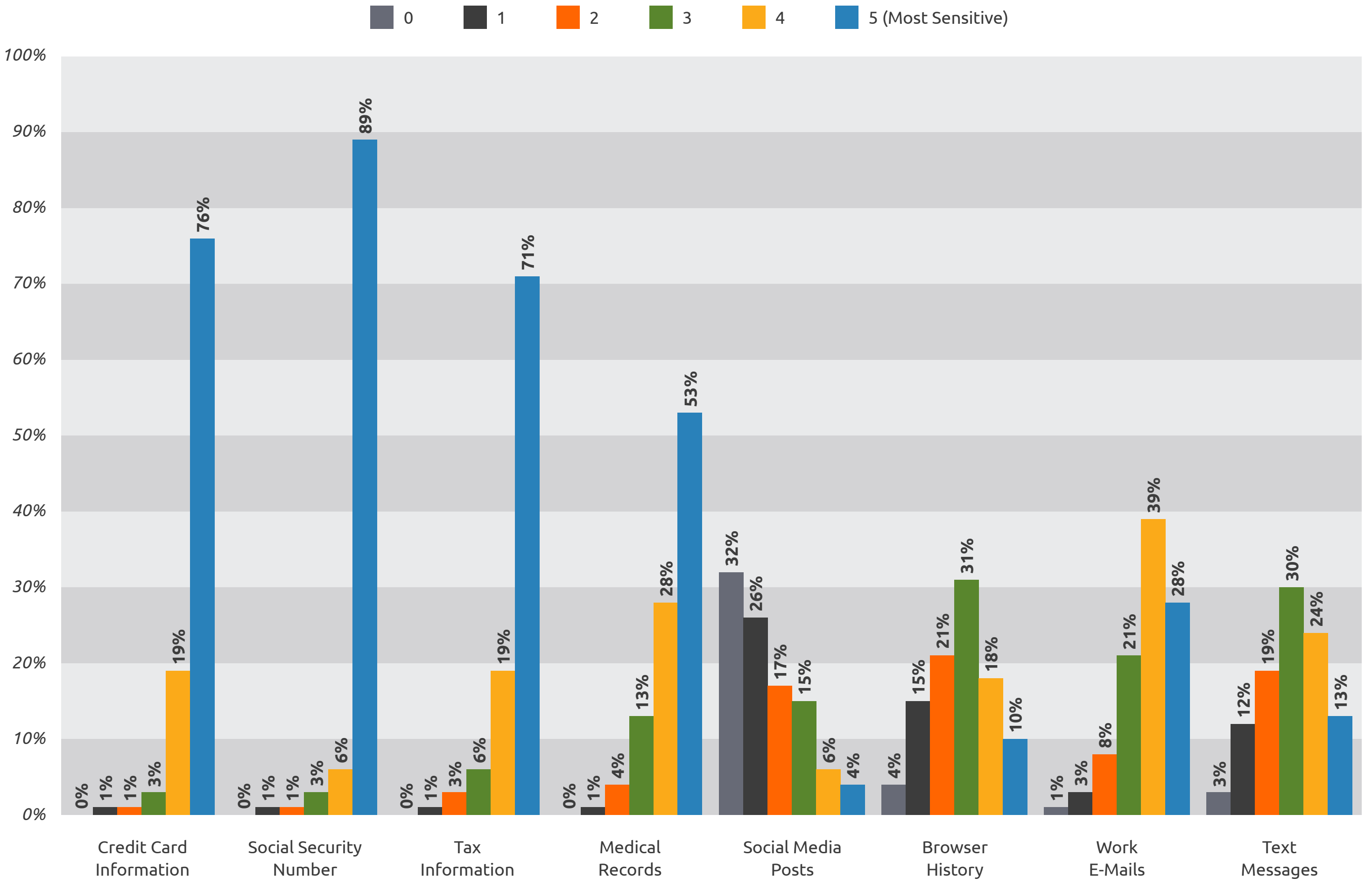
When we broke the data down by age, one main trend emerged: the older the survey respondent, the less likely they were to grant applications any of the 11 permissions (Figure 2.2) . For all but one permission (adding or modifying calendar events), a higher percentage of 55 and older respondents answered “never,” compared to the two other age groups.

SECTION 3:
DETERMINING THE SENSITIVITY OF SPECIFIC TYPES OF INFORMATION

We asked survey respondents how sensitive they thought the following types of information are, on a scale from 0 to 5 (with 5 being the most sensitive):

- Credit card information
- Social Security numbers
- Tax information
- Medical records
- Social media posts
- Browser history
- Work emails
- Text messages

FIGURE 3.1:
HOW SENSITIVE ARE THE FOLLOWING TYPES OF INFORMATION? (5=MOST SENSITIVE)

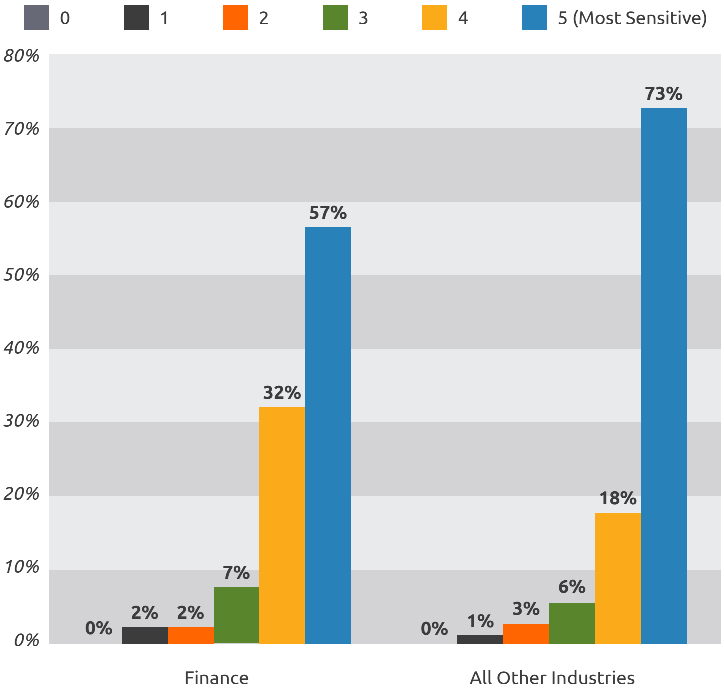


SECTION 3:
DETERMINING THE SENSITIVITY OF SPECIFIC TYPES OF INFORMATION

Overall, survey respondents judged Social Security numbers to be the most sensitive, with 89% of respondents ranking them a 5, and 6% ranking them a 4. Coming in second was credit card information, with 76% ranking it a 5, and 19% ranking it a 4. Third was tax information, which 71% of respondents ranked a 5, and 19% ranked a 4. Respondents seemed to agree that social media posts were the least sensitive type of information listed, with 58% ranking them as either a 0 or 1.

When we broke the data down by age, we found that the older the respondent, the more sensitive they considered Social Security numbers and tax information. For example, 95% of respondents 55 and older ranked Social Security numbers a 5, while 94% of 35-to 54-year-olds ranked them the most sensitive type of information. Tax information went from third most sensitive among all ages to second most sensitive among those 55 and older, with 89% ranking it a 5. Individuals 55 and older are often specifically targeted by data thieves, so it is encouraging to see that this age group realizes how sensitive social security numbers and tax information really are.

FIGURE 3.2:
HOW SENSITIVE IS TAX INFORMATION? FINANCE SECTOR VS. ALL OTHER INDUSTRIES



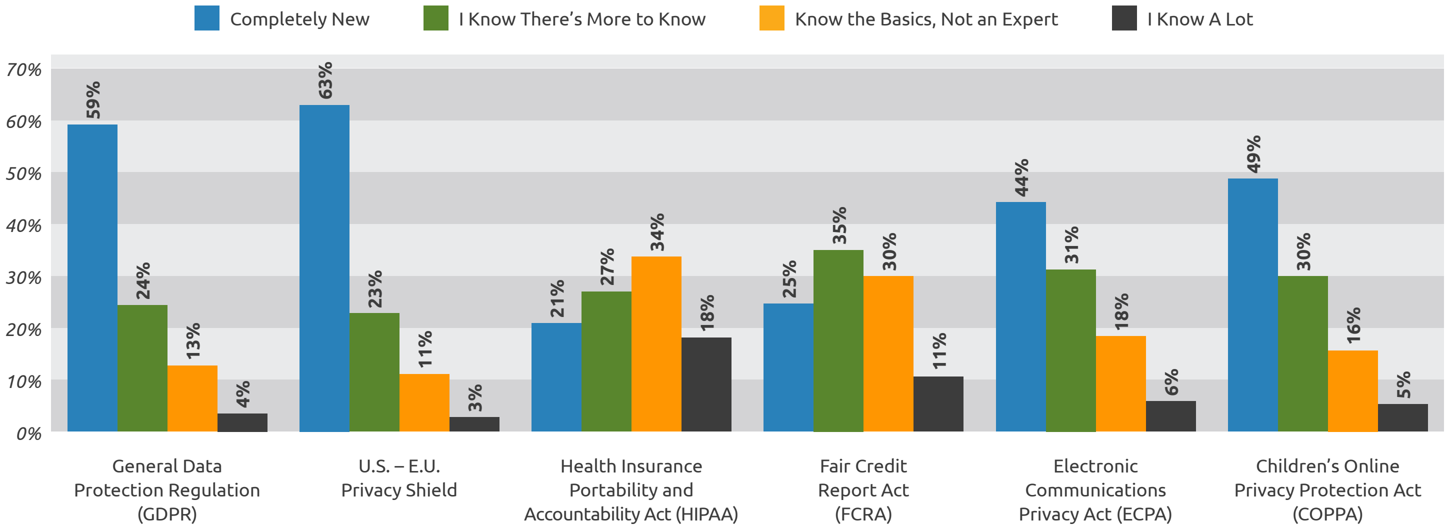
Some notable data points also revealed themselves when we broke the data down by industry. For example, financial sector employees were no more likely than other industries to rank tax information as the most sensitive type of data included in the survey. Fifty-seven percent of financial employees ranked tax information as a 5, while 73% of respondents from all other industries ranked this information as the same level of sensitivity (Figure 3.2). Similarly, respondents from the retail sector did not consider credit card information any more sensitive than did other industries. Both 94% of retail sector respondents specifically and respondents from all other industries ranked credit card information as either a 4 or a 5.

SECTION 4:
KNOWLEDGE OF NATIONAL AND GLOBAL PRIVACY REGULATIONS

We asked survey respondents how much they knew about the following six U.S. and global regulations dealing with data privacy:

- The **European Union's (EU) General Data Protection Regulation (GDPR),** which regulates how organizations, no matter their country of origin, handle and transfer the data of EU citizens.
- The **EU-U.S. Privacy Shield** regulation, which is a legal framework for transatlantic data sharing between organizations and companies in the U.S. and the EU specifically.
- The **Health Insurance Portability and Accountability Act (HIPAA),** which regulates the security of protected health information of U.S. residents.
- The **Fair Credit Reporting Act (FCRA),** which outlines the rights consumers have regarding accuracy and privacy of financial information with consumer reporting agencies.
- The **Electronic Communications Privacy Act (ECPA),** which protects electronic communications (both in-transit and stored) across email and telephone systems.
- The **Children's Online Privacy Protection Act (COPPA),** which regulates how operators of websites and online services geared toward children under 13 handle children's personal information.

FIGURE 4.1:
WHAT DO YOU KNOW ABOUT THE FOLLOWING PRIVACY REGULATIONS?

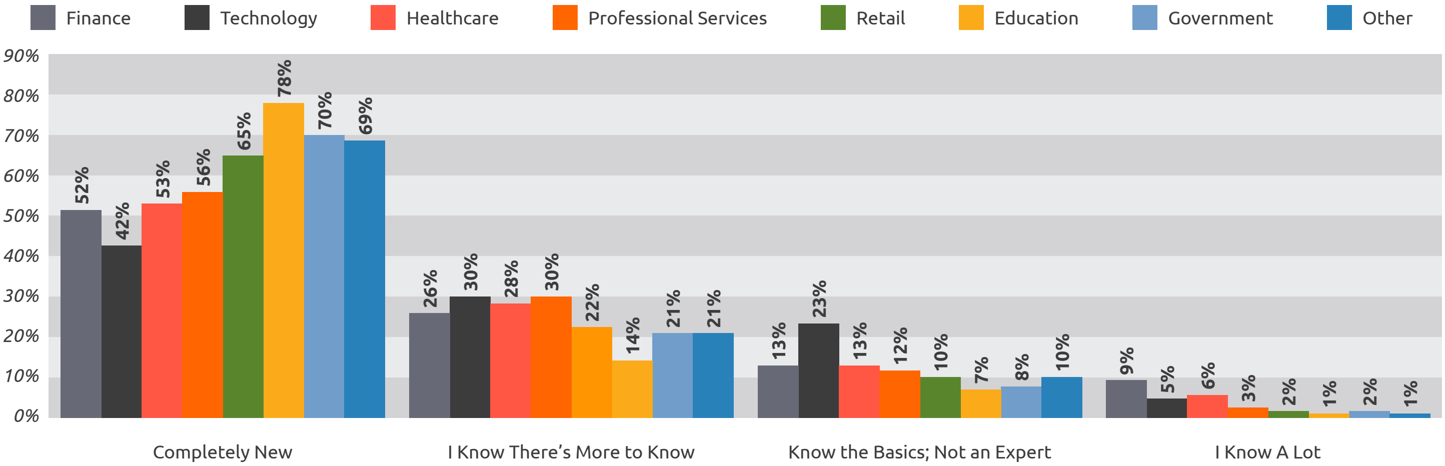


SECTION 4:
KNOWLEDGE OF NATIONAL AND GLOBAL PRIVACY REGULATIONS

Overall, survey responds were least knowledgeable about the GDPR and Privacy Shield regulations, two sets of laws dealing with the transfer of personal data across international boundaries. Sixty-three percent of respondents reported that they were completely new to the subject of Privacy Shield, while 59% said they knew little to nothing about the GDPR. A little less than a quarter of respondents reported knowing the basics of these two regulations; 24% for the GDPR and 23% for Privacy Shield.

Respondents were most familiar with HIPAA, with 52% saying they either knew the basics or were highly knowledgeable and knew what steps to take to ensure compliance. Only 21% of respondents said they were completely new to the concept of HIPAA regulations. Next, respondents were most familiar with the FCRA, with 41% reporting that they either knew the basics of the credit-reporting regulation or knew a great deal about it. A quarter of respondents reported knowing little to nothing about the FCRA. Forty-nine percent and 44%, respectively, reported knowing little about COPPA and ECPA.

FIGURE 4.2:
WHAT DO YOU KNOW ABOUT THE GDPR? BY INDUSTRY



There was no significant difference in answers between age groups. When broken down by industry, the GDPR and Privacy Shield regulations were again the first and second least known or understood, respectively. Education sector employees reported knowing the least about the GDPR, with 78% saying they were completely new to the regulation (Figure 4.2). Somewhat troublingly, respondents working for some form of government reported knowing the least about the EU-U.S. Privacy Shield regulations, with 76% revealing they were completely new to the framework of protections designed to help companies in the U.S. and Europe comply with data collection regulations in both countries.

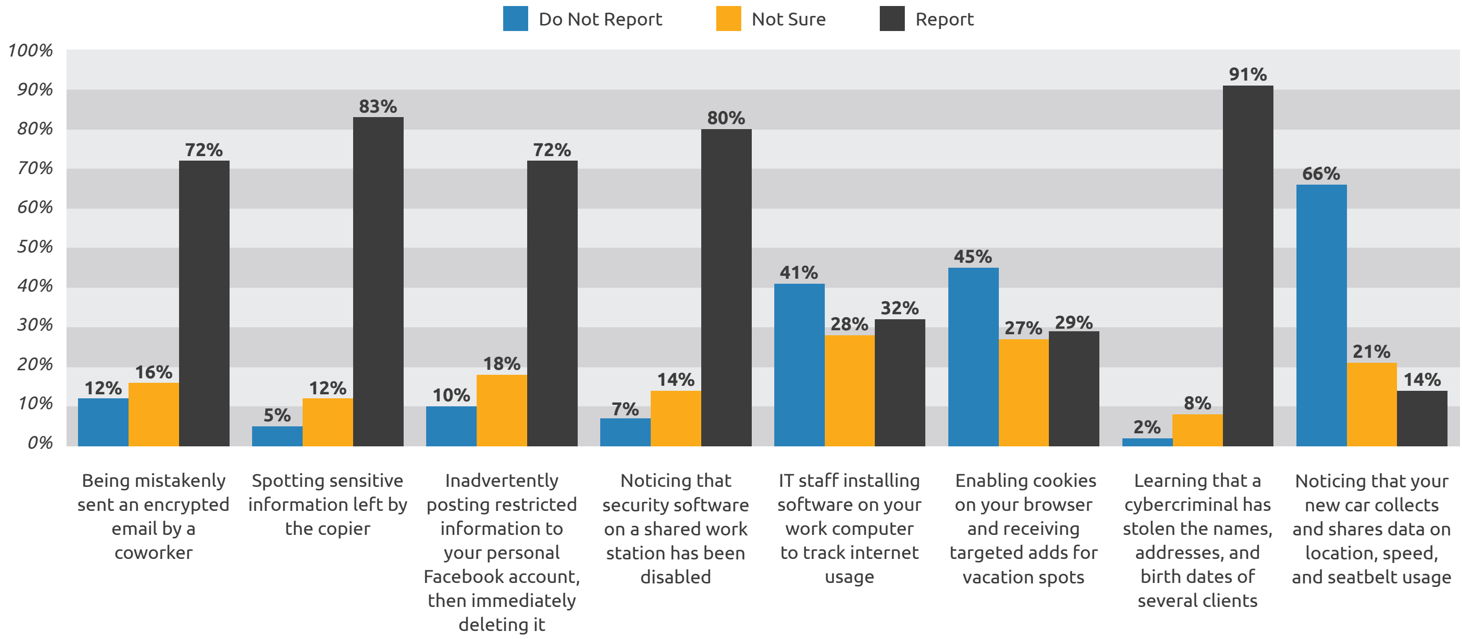
Each industry reported being the most familiar with HIPAA regulations. Understandably, a whopping 54% of healthcare industry respondents said they knew a great deal about HIPAA, by far the highest percentage of the seven industries we collected responses for.

SECTION 5:
REPORTING POTENTIAL PRIVACY INCIDENTS

We presented survey respondents with eight likely scenarios in an average work environment and asked: are these reportable privacy incidents? That is, could this incident result in the violation of federal, state, local, or company policies regarding the handling of sensitive or private information? Respondents were given three options: report, not report, or say that they were unsure what to do. The scenarios were, with correct responses included in parentheses:

- Being mistakenly sent an encrypted email by a coworker (Report)
- Spotting sensitive information left by the copier (Report)
- Noticing that security software on a shared work station has been disabled (Report)
- IT staff installing software on your work computer to track internet usage (Do Not Report)
- Enabling cookies on your browser and receiving targeted adds for vacation spots (Do Not Report)
- Inadvertently posting restricted information to your personal Facebook account, then immediately deleting it (Report)
- Learning that a cybercriminal has stolen the names, addresses, and birth dates of several clients (Report)
- Noticing that your new car collects and shares data on location, speed, and seatbelt usage (Do Not Report)

FIGURE 5.1:
WHICH SCENARIOS SHOULD BE REPORTED AS POTENTIAL THREATS TO DATA PRIVACY?

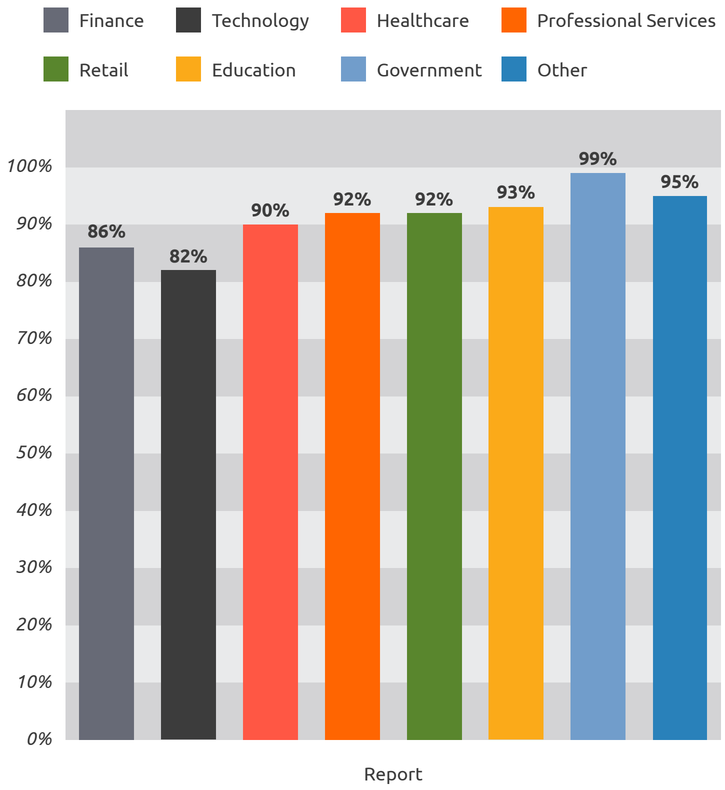


Note: The designation of a response being correct or incorrect aligns with most privacy best practices advice, though specific organizational privacy policies can vary

Respondents were generally knowledgeable on which of the above scenarios should be reported and which did not pose a threat to sensitive data. For example, 83% of respondents correctly chose to report sensitive information lying in view near a printer as a *reportable* incident. Similarly, 80% of respondents described security software on a shared work computer, a potential sign of a malware infection, as reportable.

Respondents seemed most unsure about whether IT staff installing monitoring software on a work computer and seeing targeted ads after enabling cookies on a browser were potential data privacy threats. While most (41% and 45%, respectively) correctly chose to not report these incidents, 32% and 29%, respectively, described these as reportable incidents. Though these scenarios involve the monitoring of potentially private data, they are almost always considered legitimate and are becoming more and more common in our data-driven world.

FIGURE 5.2: SHOULD YOU REPORT CYBERCRIMINALS STEALING SENSITIVE CLIENT INFORMATION AS A PRIVACY INCIDENT? BY INDUSTRY



Perhaps the most surprising result among the data was that 8% of respondents said they were unsure if a cybercriminal stealing names, addresses, and birth dates was a reportable privacy incident. An overwhelming majority (91%) correctly described such an event as reportable, though that outlying 8% still leaves room for organizations being exposed to unnecessary risk.

We discovered one main trend when we broke the figures down by industry. Across all the scenarios that would have been reportable privacy incidents, survey respondents in the technology sector were the *least likely* to identify them as such. For example, only 82% of technology sector respondents correctly chose to report cybercriminals gaining access to sensitive client information, the lowest of all the industry sectors included in the survey (Figure 5.2).

CONCLUSION

Our survey produced a mixed bag of results when it came to the data privacy knowledge of a random sampling of the U.S. populace. Some of the more positive results underscore the continued focus on proper data handling policies and procedures seen in the last few years. The powers that be seem to be realizing the importance of sound data protection procedures, albeit at the usually slow pace of regulation. The GDPR, for example, will force organizations of all types that handle EU citizen data to scrutinize their practices, or pay the price.

The results show, though, improvements should still be made to keep users more aware of how they handle sensitive data; both their own and as part of their job. This is where the concept of formalized privacy awareness training programs comes in. The designers of the GDPR, for example, realize this importance by making privacy awareness training part of the requirements. Ideally this requirement will be the prod organizations need to fold privacy awareness education into their own data privacy initiatives.

Beyond mandates from on high, though, data privacy know-how and awareness should also be considered on the microscale. We designed the scenarios in the survey to focus on the human element, rather than issues that could theoretically be handled by some technical solution or safeguard. Most put the respondent in a situation where their mistakes or inaction could be the thing that exposes sensitive information or puts it into the hands of cybercriminals. This is why data privacy cannot be considered a vague concept employees are expected to follow blindly and with no context. Such best practices need to be put in terms employees can appreciate and understand, with what's at stake clearly explained. Data privacy is everyone's responsibility and should be presented as such.

ABOUT MEDIAPRO

MediaPro creates engaging e-Learning experiences that transform behavior, improve performance, and achieve business results. We offer a suite of security awareness, privacy awareness, and compliance tools and services that are used by the most risk-aware companies in the world. We deliver award-winning awareness training courseware, reinforcement resources, and an integrated LMS solution, all available through an industry-leading SaaS-based awareness portal that offers users one-stop-shop access to every facet of their awareness program.

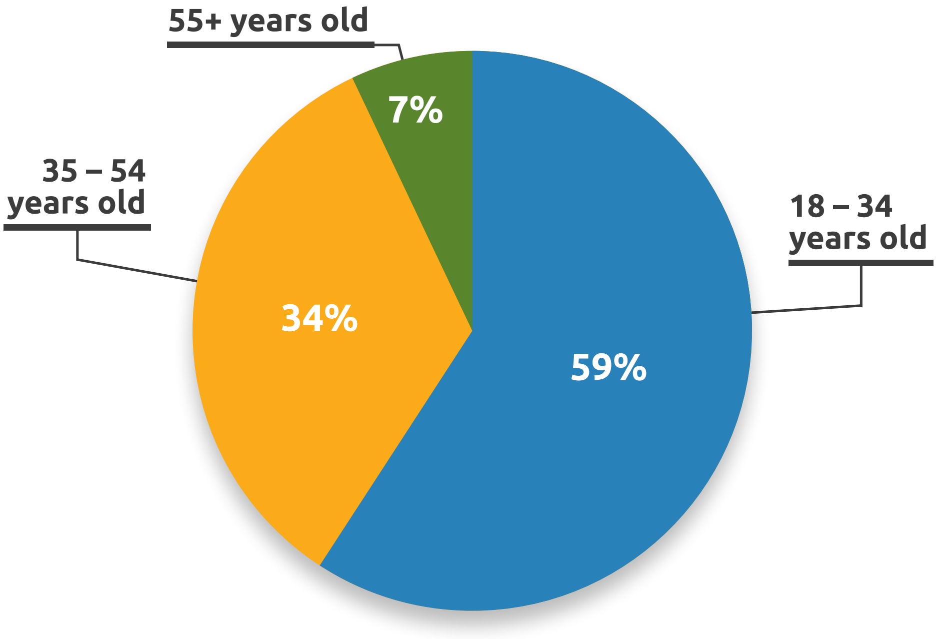
For more than two decades, MediaPro has been helping enterprises of all kinds improve the professional performance of their people. We're passionate about our work in adult learning, and it shows in the quality of our courses, the delight of our clients, and in our industry recognition.

LEARN MORE ABOUT MEDIAPRO

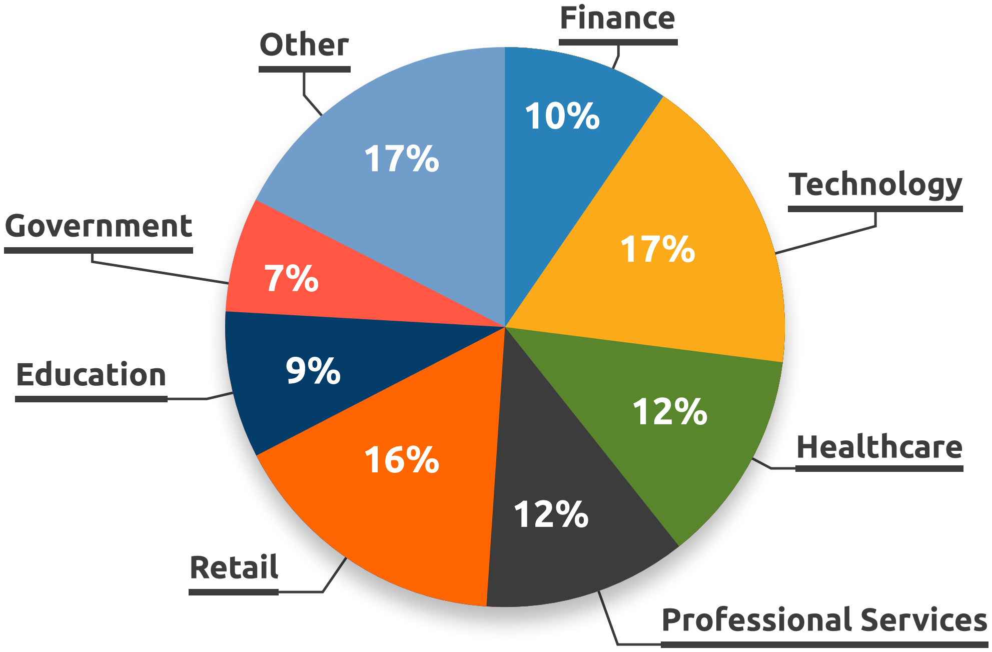
APPENDIX

The survey respondents broke down by age and industry as follows:

WHAT IS YOUR AGE?



WHAT INDUSTRY DOES YOUR ORGANIZATION BELONG TO?


Finance
Other
Technology
Government
Education
Healthcare
Retail
Professional Services