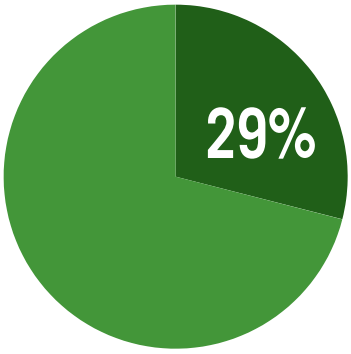
Fox Rothschild LLP
ATTORNEYS AT LAW

PRIVACY & DATA SECURITY COVID-19 IMPACT

The conversation around COVID-19 in terms of privacy and data security can be broken down into two main categories:

- The chaos leading opportunistic hackers to take advantage of our increased reliance on computers and the internet for communication.
- The privacy of personal health and location information as the U.S. government attempts to combat the novel coronavirus.

Early Industry Impact of COVID-19



Working from Home

29% of American employees have the ability to work from home. Over the last several weeks, companies are seeing a major uptick in the number of COVID-19-related cyber attacks as employees shift to working remotely.

COVID-19 Content Attacks: Hackers are increasingly creating coronavirus-related websites, apps, and tracking tools meant to lure people and then spread malicious software.

Conference Calls: Video chat software Zoom has issues with hackers who pop into and disrupt video meetings. The company was sued on April 7 by shareholders over privacy issues.

Future of Telework: As companies adapt to the new WFH requirements, the U.S. may reach a tipping point where the practice becomes more commonplace post-pandemic.

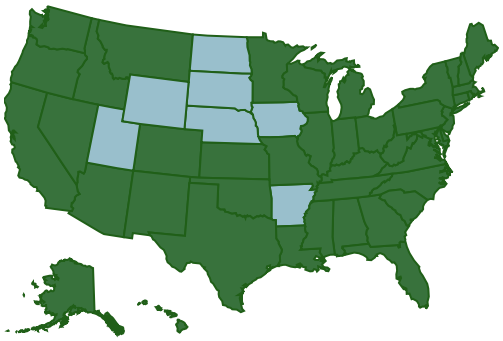
Information Tracking

Apple Inc. and Google Inc. have collaborated to develop a new system for tracking, through Bluetooth technology, the contacts of those who have tested positive for COVID-19. The tech giants stressed that they developed the method with privacy and security in mind.

Location Data: The virus' spread has prompted governments to consider use of location data culled from smartphones to notify people of a potential exposure.

Health Data: In addition to location information, this system includes tracking positive COVID-19 test results to show areas of spread.

Privacy Concerns: The move has raised concerns about what governments will do with this data and if the information can be tied to specific individuals.



Shelter in Place

All but seven states are currently observing "shelter in place" or "stay at home" orders. This accounts for 90% of the U.S. population. As a result, people are spending more time online, which can lead to higher risk of privacy and cybersecurity issues.

Telemedicine: Use of telehealth services has increased 54% from January to March 2020. Many providers are increasing their digital capabilities.

Online Schooling: School districts across the country have made the switch to online learning. Concerns over the security of Zoom has caused the NYC school district to switch to other platforms.

Online Shopping: E-commerce is vulnerable to malware attacks such as e-skimming. With consumers in their homes, online shopping has increased 52% over this time last year.

Sources: The Atlantic, CBS News, Tech Crunch, The Wall Street Journal, Law360, BigCommerce, CNBC, eMarketer

April 2020

PRIVACY & DATA SECURITY COVID-19 IMPACT

LEGAL IMPLICATIONS

GDPR

- GDPR continues to be applicable during the COVID-19 pandemic.
- Many data protection authorities, such as the European Data Protection Board, have issued guidance on how to comply. Much of the guidance highlights employees' obligations to act upon the directives of public health authorities, employers' obligations to protect their employees and how to balance public interest against privacy considerations.
- The Data Protection Agencies of certain EU member states have also issued additional guidance.

CCPA

- The CCPA went into effect January 1, 2020, but is not enforceable until July 1, 2020.
- In mid-March, a coalition of more than 60 companies across a number of industries wrote a letter to California's Attorney General requesting that the enforcement date be delayed for six months. Reasons for the request include: 1) to help alleviate the challenges recently presented by forced telecommuting and 2) to account for the lack of final CCPA-related regulations.
- As of April 15, the Attorney General's office has declined to delay the enforcement date.

HIPAA/ Telemedicine

- HHS declared a public health emergency for the entire U.S. effective Jan. 27. It also issued a limited waiver of certain provisions of the HIPAA Privacy Rule for covered hospitals effective on March 15, and retroactive as of March 1.
- Telehealth services, which can pose a HIPAA risk, have been more widely adopted as patients avoid doctor's offices. The Department of Health and Human Services, Office of Civil Rights announced it will not impose penalties for noncompliance with HIPAA for providers' good faith provision of telehealth services during the pandemic, even for services unrelated to COVID-19.

RECENT NEWS

Social Media Companies Sued

A lawsuit claims Facebook and LinkedIn have been secretly harvesting personal information from Zoom users to boost their revenues. The complaint also accuses Zoom of unlawfully disclosing users' personal information and misrepresenting it's security measures.

Employee Training

Law firms stress to clients the importance of employee training in cyber safety. Employees should be informed of standard WFH security procedures and ways to identify phishing schemes. Having designated IT personnel on alert is helpful in the event of an incident.

NYDFS Cybersecurity Deadline

Due to the COVID-19 outbreak, the New York Department of Financial Services extended its deadline for regulated entities to certify compliance with cybersecurity requirements to June 1, 2020 from the previous date of April 15, 2020.

Sources: Law360, FoxRothschild.com, NYDFS, American Medical Association, The National Law Review

April 2020