EDITORS
NORITA AHMAD American University of Sharjah, nahmad@aus.edu
PREETI CHAUHAN IEEE Senior Member, preeti.chauhan@ieee.org

NASA

2021 State of the Practice in Data Privacy and Security

Preeti S. Chauhan, IEEE Senior Member
Nir Kshetri, University of North Carolina at Greensboro

The data privacy and security landscape is changing drastically due to new laws and regulations, the COVID-19 pandemic, and other emerging trends. This article looks at the current state of these issues.

The last year has been a turning point for data privacy and security. While there were releases of new data privacy laws such as the California Consumer Privacy Act (CCPA) and New York data privacy bill, the COVID-19 pandemic has altered the premise of data privacy in ways one would not have previously imagined. The increased reliance on social media and video communication platforms to stay connected, almost complete work-from-home transition across all global organizations over the last year, and massive adoption of online commerce and home-delivery services exposed major vulnerabilities across the board that increased the risk of data security breaches.

Not only that, the monumental data collection efforts by governments, health agencies, and organizations to support contact tracing, health screening, and vaccination record tracking for public health purposes has, in fact, made people more vulnerable to theft and/or leakage of their private information. The need for public and private institutions as well as individuals at large to employ strong data security measures has never been more critical. This article goes over the state of data privacy and security in 2021, including the latest trends, best practices, and threats.

DATA PRIVACY AND SECURITY DEFINITIONS AND SCOPE

The terms *data privacy* and *security* are often used interchangeably, but they actually mean vastly different things. One's private data may or may not remain secure or unknown to unintended users. An example would be when we inadvertently leak our private information due

Digital Object Identifier 10.1109/MC.2021.3083916
Date of current version: 30 July 2021

to a lack of appropriate data security measures, such as a weak password. In general, a more convenient method to store private data also makes the user more vulnerable to data security breaches.[1]

While data privacy and security can apply to any type of data, personally identifiable information (PII) is the most often discussed. PII includes information that can help trace the identity of a person by itself or in combination with other information directly or indirectly related to the individual. The scope of PII has been evolving and expanding, from driver's licenses, Social Security numbers, addresses, and so on to online personal data, social media posts, and IP addresses, among others.

Data privacy governs how data are collected, used, archived, shared, and deleted in accordance with the law. Recently, data privacy laws have continued to be developed and implemented all around the world. For example, the European Union (EU) enacted the General Data Protection Regulation (GDPR) in 2018 to govern the collection of personal information, including phone numbers, biometric data, IP addresses, and so on. Ireland, Australia, Denmark, Norway, Canada, Portugal, France, Brazil, Switzerland, and Iceland, among other countries, have strong privacy laws with a simple focus—the right of an individual to be left alone.

Security, on the other hand, is related to how information is protected.[2] It includes technical safeguards used to ensure the confidentiality, integrity, and availability of data.[3] Let's take an example of patient data management at hospitals to understand the difference between data privacy and security. It is common for patients to share their personal information with health-care providers. If the hospital protects the data against leaks and thefts, it is maintaining both data privacy and security.

However, if the hospital sells a patient's private information to a third party without the individual's consent, that is a breach of data privacy. In such cases, security measures are not of much use since the authorities with data access are allowing the privacy invasion.[4]

DATA PRIVACY CONTROLS VERSUS DATA SECURITY

Data privacy controls limit the sharing of nonessential information and ensure data governance systems are in place. The first step of data governance is the identification of business initiatives, mapping of the personal data assets and data flow, stakeholder identification for the data governance teams, and assessment of the security and privacy readiness.

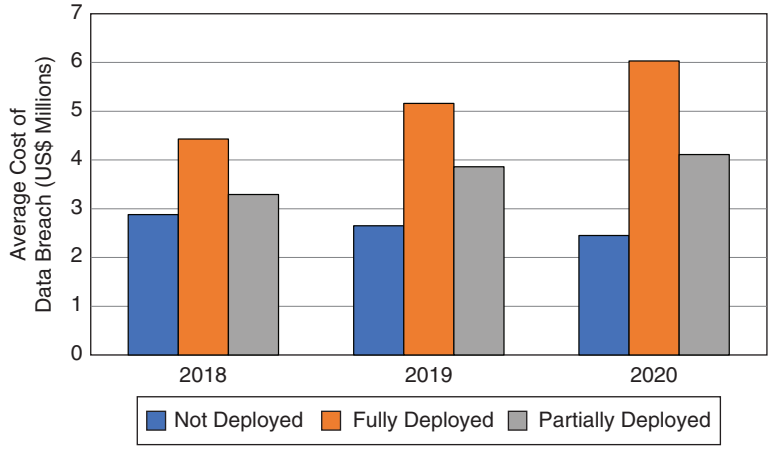

FIGURE 1. The average total cost of a data breach by security automation deployment level.[5]

The data governance team identifies risk tolerance, drives alignment on privacy policies, and develops plans for closing security gaps and data breach governance. The team also identifies any third-party vendors and associated data-sharing agreements.

In the execution phase, data assets are cataloged, and privacy policies and controls are implemented. This is also when the data subject access requests, integration of third-party vendors, and staff training on new processes takes place. The last and most important step is to measure and monitor the data governance process, course-correct as needed, and periodically test the data breach response processes.[5]

Data security tools and measures are utilized to prevent leaks and hacks of private user data. Organizations need to start by identifying the sensitive data and classifying them according to the data category and level of sensitivity. The usage policy for data needs to be set up to identify who has access to data according to data classification; the access time frame; and rules around the data usage, which should be allowed based on an individual's need to know—be it read-only or full access.

Data should be protected both physically and with endpoint security systems such as antivirus software, antispyware, pop-up blockers, and firewalls. Multifactor authentication is a very useful and powerful tool to prevent data hacks by providing a second layer of authentication for data access.[6]

An IBM study on security automation states that businesses without security automation experience an average cost of US$6.03 million in data breaches, which is more than double the average cost of US$2.45 million for companies with fully deployed security automation (Figure 1). Given the increased data security risks with remote and hybrid work environments, it is expected that the security adoption will continue to grow in 2021 and beyond.[5]

2021 STATE OF DATA PRIVACY AND SECURITY

Data privacy and security continues to evolve and has changed tremendously as a result of COVID-19 situation around the world. New macro trends of working from home, increased reliance on social media to stay connected due to lockdowns and sheltering in place, cryptocurrency growth and the resulting ransomware attacks, and so on have contributed to the emerging trends in data privacy and security risks.

Contact tracing

Contact tracing as a means to identify COVID-19 exposure risks for the community was a major initiative from governments and health agencies throughout the world. However, privacy concerns have resulted in lower adoption rates of these centralized contact-tracing tools. The applications upload the anonymized user data to a remote server, which matches the data with the user contacts, should a person start to develop COVID-19 symptoms. Besides privacy, a couple of other reasons—low GPS location precision and the discontinuation of the tracing efforts among states—severely limited the effectiveness of these tools.

The alternative technology—decentralized applications that broadcast rotating, randomized Bluetooth identifiers—has gained more traction and is also better at preserving the user's privacy. The contact-tracing collaboration by Apple and Google based on such Bluetooth identifiers has demonstrated that the data-sharing efforts can be implemented without tracking user locations or collecting PII data.

This emerging model might achieve wider adoption by other companies for non-COVID-related applications as well as to understand user preferences and activities to support their businesses. However, this will come with new privacy and data security concerns, which will need to be thought through ahead of time.

Remote/hybrid work

Remote/hybrid work has emerged as a major change owing to COVID-19 pandemic social distancing requirements. Major organizations have driven people, processes, and culture to adapt to the new reality. Some of the challenges have been to determine secured technologies to conduct confidential meetings in a remote workspace and manage confidential data outside of remote places. There are increased vulnerabilities in the form of phishing email attacks, unauthorized access through unsecured remote-access tools, hacking of video conference tools, and so on. There is a need to do periodic risk assessments, perform routine monitoring, and secure the tools enabling the remote work.

COVID-19-related medicalt and personal information

To keep the on-site business running, companies have developed new processes for COVID-19 testing as well as employee data collection to enable contact tracing. These measures enable the timely release of warnings for people who might have come in contact with a COVID-19-affected individual at the workplace. The user data collection is expected to continue throughout 2021 with the addition of the COVID-19 vaccination program. It will require organizations and companies to have systems in place to enable secure data collection, storage, and release of individuals' medical and COVID-19-related data.

Biometrics

Biometrics are physical or human characteristics that can be used to digitally identify a person, typically to give access to devices, data or systems, and so on. Examples include fingerprints, facial patterns, and voice, among others.

In 2019, the Illinois Supreme Court released Illinois's Biometric Information Privacy Act (BIPA), which states that collecting biometric information without a release or sharing the biometric information with a third party without consent would be a violation. Individuals can allege a violation of their rights to qualify as an aggrieved person and, in turn, be entitled to seek monetary compensation and injunctive relief under the act.

BIPA litigations related to biometric timekeeping-/access-related gaps have been impacted by COVID-19. Biometric data in the form of thermal scanners, facial recognition tools, and so on are being collected to have COVID-19 screening programs in place. In late 2020, there was a lawsuit filed on behalf of a company's employees, alleging that their consent was not obtained for the employer's COVID-19 screening program, which required the workers to undergo facial geometry and temperature scans to enter the company warehouses. It was alleged that the company violated BIPA by making its employees go through the above screening program, without their consent. The states of Washington, Texas, and California have similar privacy laws like BIPA, while Arizona, Idaho, Massachusetts, and New York are in the process of proposing similar legislation.[7]

Ransomware

Ransomware is a malware attack that uses asymmetric encryption to hold a user's or organization's critical data for ransom using a pair of keys to encrypt and decrypt a file. The attackers make the decryption key available to the victim upon payment, failing which the data are lost forever. While ransomware attacks used to be different from hacking, wherein the user data gets stolen, nowadays, nearly half of ransomware attacks do steal data before encrypting systems, which makes them a full cybersecurity incident.

Ransomwares have increased 62% globally and by a 158% spike in North America since 2019.[8] A large part of the dramatic rise in 2020 has been due to the work-from-home policies implemented by organizations worldwide when COVID began, which have opened up a lot of

security vulnerabilities for many organizations. In May 2021, Colonial Pipeline was held for a ransom of US$5 million by the DarkSide hacking group.[9] The company ended up paying the ransom in cryptocurrency, which has become a preferred means of ransom payment. Cryptocurrency is a virtual currency that is secured by cryptography, decentralized, and based on blockchain-distributed ledger technology, all of which allows hackers to hide their identities through the use of mixes and tumbler services.

DATA SECURITY TECHNOLOGY, TOOLS, AND TRENDS

Many organizations and individuals are devoting more resources to improving their defenses against cyberthreats. According to Juniper Research's report *The Future of Cybercrime & Security: Enterprise Threats & Mitigation 2017–2022*, global cybersecurity spending will reach US$135 billion in 2022.[10] Cybersecurity Ventures estimates even higher global cybersecurity spending: US$1 trillion for the five-year period from 2017 to 2021, or an average of US$200 billion annually.[11]

Organizations' awareness of emerging threats and several other factors have led to increased cybersecurity spending. First, major countries have issued new regulations that emphasize strong cybersecurity measures. For instance, China's Cybersecurity Law, enacted in 2017, requires financial services firms to have IT infrastructures that meet various specifications. They also need to pass standard cybersecurity tests and have certifications. Failure to comply can result in heavy fines and even criminal charges.[12]

A second factor is the shifting customer mindset. Customers expect companies to give a high priority to cybersecurity. According to "RSA Data Privacy & Security Report," based on a survey in Europe and the United States, 62% of the respondents said that they would blame the company, instead of cybercriminals, if their data were breached.[13] Finally, the evolution to a digital business strategy has stimulated cybersecurity spending.[14] Companies are gathering more data on consumers. Effective measures to secure sensitive information and maintain privacy are important to build and retain trust in brands.

Firms are deploying advanced and sophisticated tools, such as artificial intelligence (AI), machine learning (ML), and blockchain to fight cyberattacks. AI's use in cybersecurity has gained prominence in recent years. For instance, AI can analyze large numbers of documents, server logs, and other information to identify, classify, and present possible cyberthreats. Doing so is difficult and time consuming for human cybersecurity analysts. AI programs can generate real-time reports of cyberthreats, which can help the cybersecurity team to identify and resolve them quickly.[15]

However, due to challenges, such as too many false positives of AI systems, some analysts have recommended using multiple AI algorithms to fight cybercrimes. Resistant AI, a cybersecurity company in Czech Republic, uses up to five different ML modules to make a decision.[15]

Likewise, blockchain has the potential to significantly strengthen organizations' cybersecurity practices. For instance, a party can cryptographically sign transactions, and, by verifying the cryptographic signatures, the recipient can ensure that the transaction originated from a trusted source. There is no need to store sensitive information with third parties. Many interlocked computers hold identical information, and, if one computer's blockchain updates are breached, the discrepancy is noticed by all computers, and the system rejects it.

THREATS

Organizations and individuals face multiple and diverse cyberthreats. According to "The Economic Value of Prevention," a report from the Ponemon Institute, phishing, Domain Name System-based attacks, viruses, bots, distributed denial-of-service, and ransomware are among the most common types of cyberattacks facing organizations.

These attacks are growing at alarming rates. For instance, by 2019, there were about 980 million malware programs, and 350,000 new malware types were detected every day.[16] In 2019, SonicWall recorded 9.9 billion malware attacks.[17] Kaspersky Lab detected more than 482 million phishing attempts in 2018, compared to 236 million such attempts in 2017.[18]

According to the 2020 Internet Crime Report released by the U.S. Federal Bureau of Investigation's Internet Crime Complaint Center, the agency received 791,790 cybercrime complaints in 2020 compared to about 300,000 in 2019. The reported losses from cybercrime in 2020 were US$4.2 billion. The top three categories of crimes in 2020 were phishing, nonpayment/nondelivery, and cyberextortion.[19]

Increased Digitization and Social Media Use

More than 60% of the world's population is online, and 2020 marked the year in which more than half of the world's population had used social media. As of April 2021, the biggest social media company, Facebook, had 2.8 billion monthly active users.[20] Due to the huge size and high-quality information, social media is an attractive target for cybercriminals.

Social media users have been victims of high-profile privacy violations and security breaches. A study of the cloud-based email security vendor Vade Secure found that Facebook was the second-most impersonated brand in phishing attacks. Among the 25 most impersonated brands in the fourth quarter of 2019, three were social media websites.[21]

As a recent example, the media widely reported in April 2021 that a user in a hacking forum published the personal information of more than 533 million Facebook users from 106 countries. The exposed data included the phone numbers, Facebook IDs, full names, locations, birthdates, biographies, and, in some cases, email addresses of the victimized social media users.[21]

Social media companies have also been found to engage in illegal sharing

of personal information. In 2020, South Korea's information protection regulator, the Personal Information Protection Commission, fined Facebook US$6.1 million. From mid-2012 to mid-2018, Facebook allegedly shared 3.3 million South Korean users' personal information with as many as 10,000 companies without users' consent.[22]

COVID-19-Led Increase in Data Privacy and Security Risks

While broad public support existed for protective measures against COVID-19, concerns have been raised about the intrusiveness of such measures on data privacy.[23] Many COVID-19 tracking apps perform poorly in privacy and security. A study published in *Nature Medicine* in May 2020 analyzed 50 such apps, including 20 issued by government agencies in developing and developed countries. The analysis found that only 16 had indicated that they would make users' data anonymous, encrypt and secure them, and report only in an aggregated format.[24]

Likewise, an analysis by the independent watchdog agency International Digital Accountability Council (IDAC) of 108 COVID-19 apps across 41 countries found that many of the apps failed to follow best privacy and security practices.[25] IDAC's report, published in June 2020, found that many apps were using third-party software development kits, which raised the possibility that data could have been shared with outside organizations without users' consent. The apps lacked transparency about the information collected, and some failed to encrypt transmitted information.[26]

Moreover, systemic cyberrisks are posed due to remote working in the COVID-19 environment.[23] Lower safeguard standards are likely when people work from home.[12] For instance, employees working remotely may use their own devices, such as phones, laptops, and tablets. Unlike devices issued by organizations, personal devices are less likely to be patched for the latest vulnerabilities. Consumer-level systems focus more on ease of use and often lack options for customization. Enterprise-level systems, on the other hand, are designed to protect larger organizations and come with additional resources and features to strengthen security.[28]

Social control mechanisms that protect workers from dangerous cyberattacks do not operate in remote working. For instance, employees' in-person interactions with coworkers and supervisors may shield them from unsafe cyberpractices at work, which are not available in a remote working environment.[29]

DATA PRIVACY REGULATIONS

To improve the legal clarity and certainty around data privacy and strengthen cybersecurity, many jurisdictions are revamping their regulatory systems. In this section, we provide a brief overview of data privacy and security regulations worldwide.

The EU

The EU's GDPR, which is viewed as the world's most comprehensive data privacy legislation, went into effect on 25 May 2018. GDPR has made it mandatory to notify the relevant supervisory authority of any data breach within 72 h of becoming aware of the event. The number of such notifications as well as the fines imposed for privacy violations and data breaches have increased dramatically (Figure 2).

Many new privacy laws have been inspired, at least in part, by GDPR, which has dramatically changed the processes that organizations need to follow to track consumers' online behaviors and process that data. Under GDPR, companies are required to obtain specific legal bases to use customers' data or track their behaviors. Many companies choose consent as the legal basis.[31] GDPR requires companies to have an explicit opt-in consent from customers to keep personal data.

In a context of international comparison, GDPR's Article 45 is of special interest; it gives the European Commission (EC) the power to determine whether a country outside the EU provides an adequate level of data protection. If a non-EU country meets the adequacy standard, data flow from the EU to that country is treated in the same manner as intra-EU transmissions of data.[32]

The United States

Compared to the EU, the United States provides more autonomy to businesses regarding the way they disclose and store personal information. Organizations' data privacy and security frameworks are subject to a number of federal laws and regulations enacted to protect the privacy, security, and confidentiality of specific categories of data and information. In addition to federal laws, there are about 47 different state laws regarding how people should be notified in the case of a data breach involving personal information.[33]

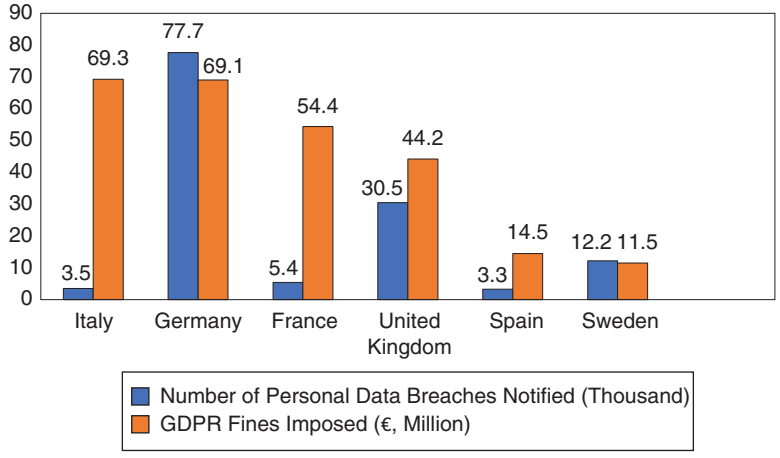

FIGURE 2. The top six economies imposing GDPR fines (25 May 2018 to 27 January 2021).[30]

Among most notable state-level legislation in the United States, the CCPA became effective on 1 January 2020. It is largely modeled after GDPR but is less stringent. Both GDPR and the CCPA strongly emphasize transparency. For example, to comply with the CCPA, a business is required to include a section in its privacy policy that describes the rights of consumers. It must provide clear instructions regarding how consumers can opt out of the sale of their personal information.

In November 2020, the California Privacy Rights Act (CPRA) was passed, which will replace and build on the CCPA. The CPRA will take full effect in 2023 and will give users new rights, such as the right to correct inaccurate information, right to have personal information collected subject to data minimization and purpose limitations, and right to receive notice from businesses planning on using sensitive personal information and ask them to stop.[34]

Among other U.S. states, Virginia's governor signed the Consumer Data Protection Act (CDPA) into law in March 2021, which will take effect January 2023. Like the CPRA, the CDPA requires companies to publish privacy policy notices that explain the ways they use, collect, and share personal data. Without consumers' affirmative consent, companies cannot collect and process their personal data. The CDPA also gives individuals the right to ask whether a company is storing and processing their personal information. In addition, they can request the deletion and correction of their personal data. Virginia consumers also have the right to opt out of the sale of their personal data as well as the use of such data to create targeted advertising.[35]

Asia

As of May 2021, Japan was the only Asian country that was granted an Adequacy Decision by the EC. South Korea enacted the Personal Information Protection Act (PIPA) in 2011. In addition, the country has sector-specific data privacy legislation.[36] The PIPA requires private- and public-sector entities collecting information that identifies a specific person to meet strict compliance requirements.[37]

In China, the 2012 Online Data Protection Regulation bans the sale and distribution of personal information without the owner's consent. It requires Internet service providers to ensure the security of personal data and prevent misuse as well as provides consumers the right to seek the deletion of personal data posted without consent and sue for violations. However, the Chinese government's state power allows it to get unlimited access to citizens' personal information for surveillance.[38]

As of April 2021, India lacked a comprehensive data privacy law to protect personal data. In December 2019, India's lower house of the bicameral parliament, Lok Sabha, introduced the Personal Data Protection Bill, 2019. It specifies how the data of Internet users are stored, processed, and transferred. The bill was tabled as of April 2021.[39]

Latin America

After GDPR's implementation, significant amendments and improvements in privacy laws were made by major Latin American countries. As of May 2021, the EC had recognized Argentina and Uruguay as jurisdictions that provide adequate protection. Argentina changed its data protection laws enacted to align with GDPR. In 2018, a bill was proposed that contains key provisions of GDPR, such as a requirement for governmental agencies processing sensitive and big data to appoint a data protection officer and standards for the lawfulness of data processing.[40] Likewise, the Brazilian General Data Protection Law (Lei Geral de Proteção de Dados) was ratified in the Congress in mid-2018 and became effective on 18 September 2020.

Africa

In most countries in Africa, underdeveloped regulatory regimes fail to provide adequate data privacy protection. As of early 2021, about half of Africa's 53 countries had adopted some form of data privacy regulations.[41] Likewise, in 2014, the African Union's convention on cybersecurity and personal data was adopted. As of May 2021, 14 nations had signed it, and eight had ratified and/or accessed the conventions.[27]

Data privacy and security are and will continue to cause an evolving conversation around the world. The increased threats of data leakages and thefts from high digitization and social media usages as well as new vulnerabilities resulting from the hybrid work culture need to be continuously monitored and addressed.

The complexities around privacy require action and active participation from individuals, businesses, and government agencies. It is important to improve legal clarity and certainty around data privacy and security through regulations at the state and federal levels in the United States as well as around the world.

At the individual and business levels, it is necessary to remain cognizant of cybersecurity threats and vulnerabilities and actively work to address these with advanced and sophisticated tools, such as AI, ML, and blockchain, to improve privacy controls and ward off cyberattacks. In these unprecedented times, the definition, scope, and impact of data privacy and security have gone through tremendous changes, and it will require individual, corporate, and government actions to ensure that the user data are handled in a manner that does not compromise privacy and security. C

ACKNOWLEDGMENT

We thank *Computer*'s editor in chief, Jeff Voas, for suggestions on a previous version of this article.

DISCLAIMER

The views, thoughts, and opinions expressed in the article belong solely to the authors, and not necessarily to their employer or organizations, committees, or groups that the authors may be a part of.

REFERENCES

1. S. Ritter. "Data privacy Vs. data secrecy: The danger of worrying about the wrong issue." Forbes, Sept. 3, 2019. https://www.forbes.com/sites/forbestechcouncil/2019/09/03/data-privacy-vs-data-secrecy-the-danger-of-worrying-about-the-wrong-issue/?sh=3fe3585b3ce9
2. S. Symanovich. "Privacy vs. security: What's the difference?" Norton, Jan. 18, 2020. https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html (accessed Mar. 20, 2021).
3. K. Schwartz. "Data privacy and data security: What's the difference?" IT-Pro Today, May 2, 2019. https://www.itprotoday.com/security/data-privacy-and-data-security-what-s-difference (accessed Mar. 20, 2021).
4. L. O. Gostin, "Health information privacy," *Cornell Law Rev.*, vol. 80, no. 3, pp. 451–528, 1995.
5. F. Velez. "What's in store for data privacy in 2021?" CPO Magazine, Jan. 18, 2021. https://www.cpomagazine.com/data-privacy/whats-in-store-for-data-privacy-in-2021/ (accessed Mar. 2, 2021).
6. "9 data security best practices for 2021." Team LoginRadius, Dec. 09, 2020. https://www.loginradius.com/blog/start-with-identity/2020/12/data-security-best-practices/ (accessed Mar. 20, 2021).
7. M. T. Costigan. "Top 10 for 2021 – Happy data privacy day!" Workplace Privacy Report, Jan. 28, 2021. https://www.workplaceprivacyreport.com/2021/01/articles/written-information-security-program/top-10-for-2021-happy-data-privacy-day/ (accessed Mar. 20, 2021).
8. C. Matthews. "Bitcoin extortion: How cryptocurrency has enabled a massive surge in ransomware attacks," MarketWatch, May 15, 2021. https://www.marketwatch.com/story/bitcoin-extortion-how-cryptocurrency-has-enabled-a-massive-surge-in-ransomware-attacks-11621022496 (accessed Mar. 20, 2021).
9. "Ransomware soars with 62% increase since 2019," Security Magazine, Mar. 16, 2021. https://www.securitymagazine.com/articles/94831-ransomware-soars-with-62-increase-since-2019#:~:text=Ransomware%20reaches%20new%20heights%20with,to%20earn%20an%20easy%20payday (accessed Mar. 20, 2021).
10. "Cybercrime & the internet of threats 2018," Juniper Research, 2017. https://www.juniperresearch.com/whitepapers/cybercrime-the-internet-of-threats-2018 (accessed Mar. 20, 2021). (accessed Mar. 20, 2021).
11. B. Sterling. "Global cybercrime. Costs a trillion dollars Maybe 3." Wired, July 19, 2017. https://www.wired.com/beyond-the-beyond/2017/07/global-cybercrime-costs-trillion-dollars-maybe-3/ (accessed Mar. 20, 2021).
12. N. Kshetri, *Cybersecurity Management: An Organizational and Strategic Approach*. Toronto: The Univ. of Toronto Press, 2021
13. M. Nadeau. "General Data Protection Regulation (GDPR) requirements, deadlines and facts." CSO, 2018. https://www.csoonline.com/article/3202771/data-protection/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html (accessed Mar. 20, 2021).
14. "Gartner forecasts worldwide security spending will reach $96 billion in 2018, up 8 percent from 2017." Gartner, 2017. https://www.gartner.com/en/newsroom/press-releases/2017-12-07-gartner-forecasts-worldwide-security-spending-will-reach-96-billion-in-2018 (accessed Mar. 20, 2021).
15. J. Kahn. "Cybercriminals adapt to coronavirus faster than the A.I. cops hunting them." Fortune, Apr. 30, 2020. https://fortune.com/2020/04/30/cybercriminals-adapt-to-coronavirus-faster-than-the-a-i-cops-hunting-them (accessed Mar. 20, 2021).
16. B. Jovanović. "Malware statistics – You'd better get your computer vaccinated." DataProt. 2019. https://dataprot.net/statistics/malware-statistics/ (accessed Mar. 20, 2021).
17. "2020 Sonicwall cyber threat report: Threat actors pivot toward more targeted attacks, evasive exploits." Sonicwall, San Jose, CA, Feb. 4, 2020. [Online]. Available: https://www.sonicwall.com/news/2020-sonicwall-cyber-threat-report/
18. "Phishing attacks more than doubled in 2018 to reach almost 500 million." Kaspersky, 2019. https://www.kaspersky.com/about/press-releases/2019_phishing-attacks-more-than-doubled-in-2018 (accessed Mar. 20, 2021).
19. "FBI Releases the internet crime complaint center 2020 internet crime report, including COVID-19 scam statistics," FBI National Press Office, Washington, D.C., Mar. 17, 2021. [Online]. Available: https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics
20. Q. Wong. "Facebook says iPhone users will start seeing new privacy prompt today." CNET, Apr. 26, 2021, https://www.cnet.com/news/facebook-says-iphone-users-will-start-seeing-new-privacy-prompt-today/ (accessed May 20, 2021).
21. A. Holmes. "533 million Facebook users' phone numbers and personal data have been leaked online." Business Insider. Apr. 3, 2021, https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4 (accessed May 20, 2021).
22. S. Ikeda. "South Korean regulator fines Facebook for privacy violations; social media giant shared personal data without user consent," CPO Magazine, Dec. 3, 2020. https://www.cpomagazine.com/data-privacy/south-korean-regulator-fines-facebook-for-privacy-violations-social-media-giant-shared-personal-data-without-user-consent/ (accessed May 20, 2021).

23. D. Mikkelsen, H. Soller, and M. Strandell-Jansson, "Privacy, security, and public health in a pandemic year," McKinsey & Company, New York, June 15, 2020. [Online]. Available: https://www.mckinsey.com/business-functions/risk/our-insights/privacy-security-and-public-health-in-a-pandemic-year
24. T. Sharma and M. Bashir, "Use of apps in the COVID-19 response and the loss of privacy protection," *Nature Med.*, vol. 26, no. 8, pp. 1165–1167, May 26, 2020. [Online]. Available: https://www.nature.com/articles/s41591-020-0928-y. doi: 10.1038/s41591-020-0928-y.
25. E. Reuter. "Report: COVID-19 apps fall short in privacy, security." Med City News, June 8, 2020. https://medcitynews.com/2020/06/report-many-covid-19-apps-fall-short-in-privacy-security/ (accessed May 20, 2021).
26. "Privacy in the age of COVID: An IDAC investigation of COVID-19 apps," Digital Watchdog, June 5, 2020. https://digitalwatchdog.org/wp-content/uploads/2020/06/IDAC-COVID19-Mobile-Apps-Investigation.pdf (accessed May 20, 2021).
27. "List of countries which have signed, ratified/acceded to the African Union Convention on Cybersecurity and Personal Data Protection." https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (accessed May 20, 2021).
28. J. Kelly. "Consumer vs. enterprise security: There is a difference." Law Technology Today, Sept. 5, 2019. https://www.lawtechnologytoday.org/2018/09/consumer-vs-enterprise-security/ (accessed May 20, 2021).
29. J. Boehm, J. Kaplan, and N. Sportsman "Cybersecurity's dual mission during the coronavirus crisis," McKinsey & Company, New York, Mar. 25, 2020. [Online]. Available: https://www.mckinsey.com/business-functions/risk/our-insights/cybersecuritys-dual-mission-during-the-coronavirus-crisis?cid=other-eml-alt-mip-mck&hlkid=34fdd9f7b5154c8d88ee3d25ac6cfd3f&hctky=2762145&hdpid=ffacc134-7120-4a94-ba44-bd4b2fe75bcc
30. "DLA Piper GDPR fines and data breach survey: January 2021." DLA Piper. https://www.dlapiper.com/en/uk/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/
31. D. Meyer. "GDPR attacks: First Google, Facebook, now activists go after Apple, Amazon, LinkedIn." ZDNet. May 29, 2018. https://www.zdnet.com/article/gdpr-attacks-first-google-facebook-now-activists-go-after-apple-amazon-linkedin/ (accessed May 20, 2021).
32. "Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection," European Commission, Brussels, Belgium. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed May 20, 2021).
33. R. King. "New EU cyber security directive to impact U.S. companies." The Wall Street Journal, Feb. 7, 2013. http://tinyurl.com/cjujzgl (accessed May 20, 2021).
34. "California privacy rights act: An overview." Privacy House Clearing House, Dec. 10 2020. https://privacyrights.org/resources/california-privacy-rights-act-overview (accessed May 20, 2021).
35. A. Nicodemus. "More than a CCPA clone? Virginia passes nation's second comprehensive privacy law." Compliance Week, Mar. 3, 2021. https://www.complianceweek.com/data-privacy/more-than-a-ccpa-clone-virginia-passes-nations-second-comprehensive-privacy-law/30104.article (accessed May 20, 2021).
36. "Data protection laws of the world: South Korea." DLA Piper. https://www.dlapiperdataprotection.com/index.html?t=law&c=KR (accessed May 20, 2021).
37. H. Chan. "Pervasive personal data collection at the heart of South Korea's COVID-19 success may not translate," Thomson Reuters. Mar. 25, 2020 https://blogs.thomsonreuters.com/answerson/south-korea-covid-19-data-privacy/
38. E. Feng, "In China, a new call to protect data privacy," NPR, Washington, D. C., Jan. 5, 2020. [Online]. Available: https://www.npr.org/2020/01/05/793014617/in-china-a-new-call-to-protect-data-privacy
39. A. Chakravarty and A. Sivasubramanian. "The Privacy question in India's drone regulation." Jurist, Apr. 14, 2021. [Online]. Available: https://www.jurist.org/commentary/2021/04/chakravarty-sivasubramanian-privacy-drone/
40. M. Egan, "Data privacy reform gains momentum in Latin America," IDB, New York, Feb. 12, 2019. [Online]. Available: https://blogs.iadb.org/conocimiento-abierto/en/data-privacy-reform-gains-momentum-in-latin-america/
41. J. Daniel. "Data protection laws in Africa: What you need to know." CIO, Feb. 14, 2021. https://www.cio.com/article/3607734/data-protection-laws-in-africa-what-you-need-to-know.html (accessed May 20, 2021).

PREETI S. CHAUHAN is a technical program manager at Google, Sunnyvale, California, 94089, USA. She is a Senior Member of IEEE. Contact her at preeti.chauhan@ieee.org.

NIR KSHETRI is a professor of management in the Bryan School of Business and Economics at the University of North Carolina at Greensboro, Greensboro, North Carolina, 27412, USA. Contact him at nbkshetr@uncg.edu.