CONSUMER ACTION NEWS

www.consumer-action.org • Spring 2018

Consumer Action
1170 Market Street, Suite 500
San Francisco, CA 94102

Non-Profit Org.
U.S. Postage
PAID
San Francisco, CA
Permit # 10402

Change Service Requested

Data protection issue

Data insecurity

Intrusions, breaches erode consumer privacy

By Monica Steinisch

When it comes to your personal data—name, birthdate, account number, Social Security number, etc.—landing in the wrong hands or being used in ways you wouldn't expect, it's no longer a matter of *if*, but *when*. Data breaches are a daily occurrence. Even in the absence of a breach, anyone who takes advantage of 21st century technology (think smartphones or other products that connect to the internet) forfeits some of his or her personal data every day, with little likelihood of knowing exactly who is getting it or how it's being used.

So where does that leave consumers who are required to expose their personal information as a condition of participating in the connected world?

Routine but risky

Even something as routine as driving a car has transitioned to a data-collecting event. Predictions are that over 380 million connected cars will be on the road by 2021. The data these cars generate cover everything from vehicle diagnostics and driving habits (braking, speed, etc.) to location and entertainment choices. The data offer drivers things like service notifications and on-board navigation, but also open them up to unwelcome privacy risks.

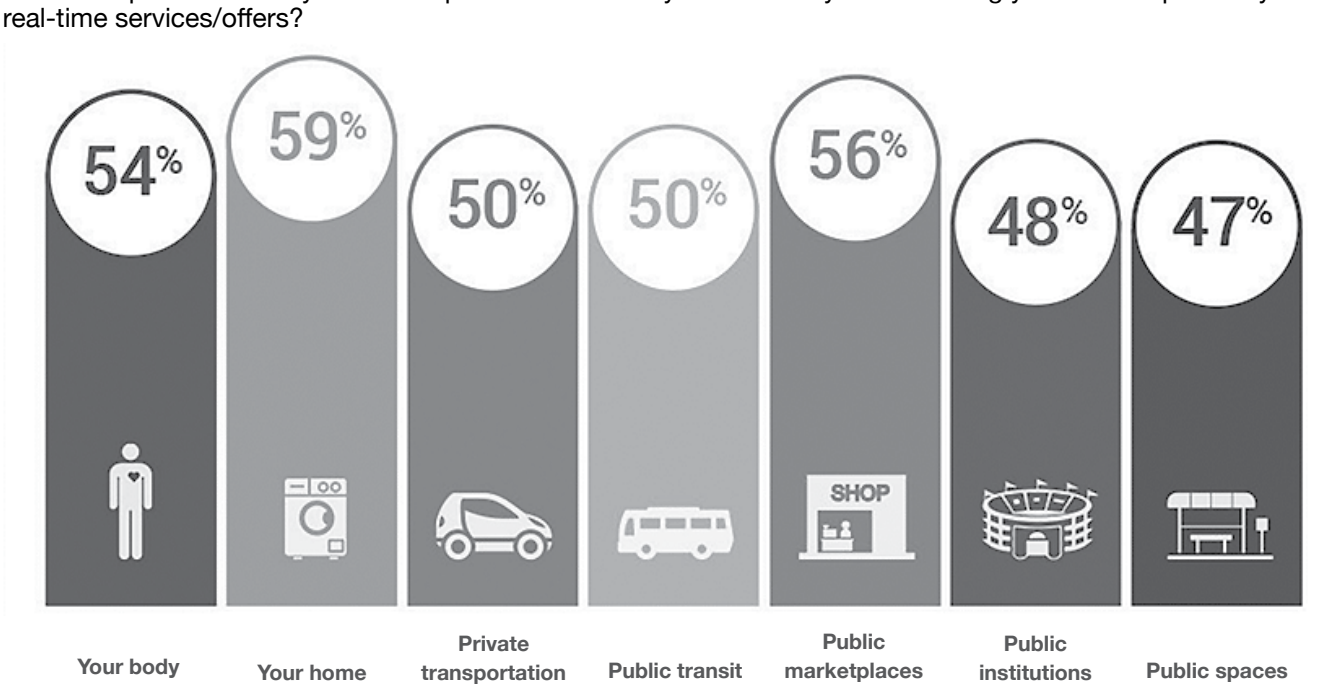
One concern is the vulnerability of customer data collected by rental cars. On-board navigation and infotainment systems gather and store personal data such as trip history, phone identifiers (Bluetooth connectivity), music streaming account information, hands-free calling history and more. This data may be ripe for access by future rental car customers, buyers of the data if rental car companies sell it, or unknown others.

There's debate over who owns and controls this customer data: rental car companies, carmakers or individual drivers? A coalition of public interest groups (including Consumer Action) has called on car rental companies and auto manufacturers to protect the privacy of driver and passenger data. One concern they raise: It's possible to track people down by analyzing the digital "crumbs" they leave behind. The coalition shared the real-life example of a Baltimore car owner who tracked down the teens who took his car for a joy ride by cross-referencing (on Instagram) the teens' phone

"Insecurity" continues on page 2

Consumers place high importance on notification of data collection

Q. How important is it to you for companies to NOTIFY you when they are collecting your data to provide you real-time services/offers?



Source: Consumer Perceptions of Privacy in The Internet of Things, Altimeter Group, June 2015

New data protection rights…for Europeans

By Ruth Susswein

European consumers will have new rights to better control their personal information online. The new rules will affect all companies—here and abroad—that do business within the European Union (EU).

Starting this May, the General Data Protection Regulation (GDPR) will help protect the personal data collected about EU citizens. However, there's hope that these protections will ultimately impact all consumers. The rules are designed to provide consumers with:

- Better access to their personal information,
- Improved corporate accountability for data handling, and
- Steeper fines for violations.

Under these rules, "personal data" is defined as information that can identify a person, such as their name, address, Social Security number, date of birth, account numbers and IP address, but it also includes "sensitive data," such as a person's location, health and genetic data, sexual orientation, and religious and political beliefs. Some of the most sensitive information will require consumers' explicit consent to be used/shared.

EU consumers will have the right to know, limit, delete and correct information related to them. Here are the new rights.

EU data protection rights

Right to know: When personal information is requested or received, consumers must be given notice about the type of data that is collected, who is using their data and for what purpose. They're also entitled to know how long the data will be retained and how it is being protected. Notice must be given clearly and concisely.

Right to access: EU consumers will have the right to access their personal information for free, whether collected directly from them or by a third party. Consumers should receive a response to their data request within 30 days.

Right to rectify: If information is inaccurate or incomplete, consumers can require that the data be corrected (or deleted), and that corrections be sent to third parties, where possible. Consumers must be told which third parties received the incorrect data.

Right to delete (be forgotten): Consumers can request that personal data be deleted or "erased"

"Europeans" continues on page 4

Consumer Action

www.consumer-action.org

Consumer Action has been a champion of underrepresented consumers nationwide since 1971. A non-profit 501(c)(3) organization, Consumer Action focuses on financial education that empowers low- and moderate-income and limited-English-speaking consumers to financially prosper.

By providing financial education materials in multiple languages, a free national hotline and ongoing financial services research, Consumer Action helps consumers assert their rights in the marketplace and make financially savvy choices.

Advice and referral hotline

Submit consumer complaints to our hotline:
http://bit.ly/CA_hotline_ENG
(415) 777-9635
Chinese, English and Spanish spoken

San Francisco

1170 Market Street, Suite 500
San Francisco, CA 94102
(415) 777-9648
Email: info@consumer-action.org

Ken McEldowney
Executive Director

Michael Heffer
Business Manager

Kathy Li
Director, San Francisco (SF) Office

Nani Susanti Hansen
Associate Director, SF Office

Audrey Perrott
Director, Strategic Partnership

Monica Steinisch
Senior Associate, Editorial

Jamie Woo
Community Outreach Manager

Joseph Ridout
Consumer Services Manager

Cui Yan Xie
Project Associate

Vickie Tse
Development Coordinator

Hazel Kong
Administrative Associate/
Consumer Advice Counselor

Angela Kwan
Web Manager

Ricardo Perez
Mail Room Operations

Rose Chan
Consumer Advice Coordinator

Schelly Gartner, Tasneem Pitalwala, Ralph Stone
Consumer Advice Counselors

Alden Chan, Robert La, Michelle Liu
Support

Los Angeles

(213) 624-4631

Nelson Santiago
Community Outreach Manager

Linda Williams
Community Outreach & Training Manager

Washington, DC

(202) 544-3088

Linda Sherry
Director, National Priorities

Ruth Susswein
Deputy Director, National Priorities
(Editor, *Consumer Action News*)

Lauren Hall
Associate, National Priorities

Alegra Howard
Associate, National Priorities

Consumer Action News is printed by the Dakota Printing Company. We use Bitly.com to shorten lengthy URLs.

Research by Finn Myrstad and colleagues at the Norwegian Consumer Council found that strangers can easily seize control of kids' smartwatches and use them to track and eavesdrop on children. (Photo: Forbrukerradet)

Insecurity

Continued from page 1

device names that were stored in his Jeep's infotainment system.

Others worry that all this auto data collection could make it too easy for hackers to access our cars' computers, and wonder what they might do with the data, or worse, with remote control of the vehicle.

Privacy and security threats posed by "connected" household objects became a frequent headline around the holidays, just as parents were shopping for "smart" toys. Advocates had complained to the FTC in 2016 about internet-connected toys whose cameras and microphones record children yet fail to prevent intruders from spying on or tracking a child.

Following research by the Norwegian Consumer Council that uncovered serious security and privacy flaws in "smartwatches" for children, the Consumer Federation of America asked the FTC to protect kids from risks associated with the watches. These devices are promoted as a tool for parents to monitor their children, but they store collected data insecurely and may allow access to the watch's microphone, camera, and location information that can "easily be overtaken by a hacker who might prey upon the child."

"It's very serious when products that claim to make children safer instead put them at risk because of poor security and features that do not work properly," says Finn Myrstad, the director of digital policy at the Norwegian Consumer Council who spearheaded the smartwatch research (http://bit.ly/2C8JlWt).

Others have called out the intrusiveness of "digital assistants"—think Siri, Google Home and Alexa. Privacy advocates predict that manufacturers will piece together detailed personal profiles to target members of the household with marketing pitches. Others see these data dossiers being used in more troubling ways, possibly by insurance companies that partner with data gatherers to incorporate the information into their decision-making and, in some cases, deny coverage or claims. Others fear that hackers could use these devices to remotely disable locks and security systems in our homes (http://nyti.ms/2Hw60LS).

Just last month, Consumer Reports' testing found that some of the biggest brands of "smart TVs" are susceptible to remote control by hackers (http://bit.ly/2GxKRjf).

Endless breaches

Even if you managed to dodge the 2013 Target Stores breach that compromised the data of up to 110 million consumers, or the 2014 cyber attack that exposed 145 million eBay accountholders, you were almost certainly one of the 145 million consumers who got snared in last year's Equifax data breach. 2017 was the "worst year ever" for personal data breaches, according to the Online Trust Alliance (http://bit.ly/2EWiNc7).

What can sting nearly as much as having your data stolen is having the company responsible conceal the breach. Take the 2016 Uber breach affecting 57 million customers: After hackers stole its customers' information, Uber paid the hackers $100,000 to destroy the data and keep news of the breach from going public.

Out of the Uber breach came word that Unroll.me, a company that unsubscribes users from unwanted email advertising, had sold its customers' anonymized Lyft ride data (taken from Lyft receipts in users' in-boxes) to Uber. This was news to Unroll.me users.

The company's privacy policy disclosed that Unroll.me "may collect, use, transfer, sell, and disclose non-personal information for any purpose," but customers, not surprisingly, felt misled. While not technically a breach, the episode serves as a reminder that a core element of many third-party apps and online services is trading in consumer data.

There's a limit to what you can do to protect your personal data and privacy. While you can secure your home's Wi-Fi network to help keep intruders at bay, the security of data stored in the cloud, as many devices require, is out of your control.

What you can do

Savvy car rental customers can reduce their risks by deleting their data from a car's infotainment system before returning the vehicle—if they know how.

Likewise, you may have some say in what data can be collected by the apps you use.

Check the settings in the app (not the device). If an app wants more personal data than you're comfortable giving up, don't download it.

Delete apps you don't use, and visit the company's website to see if your account can be deleted entirely. But be aware that some accounts simply can't be deleted, and others can only be removed after you've jumped through a series of hoops.

In reality, to date it's been virtually impossible to avoid intrusion. Companies have, in many cases, given themselves the non-negotiable right to collect and use consumers' data.

Push for privacy

Because individual consumers have such little leverage, advocates have been making the case that there are consequences to not taking privacy and safety seriously. Largely as a result of advocates' 2016 complaint, the FTC announced a settlement with toymaker VTech in January. VTech had collected information from children without parental consent, which is required under the Children's Online Privacy Protection Act.

In a long-range effort, Consumer Reports has launched the Digital Standard—digital privacy and security guidelines to evaluate mobile and internet-connected products. The objective is to influence the design of internet-connected products so that consumers' data security and privacy are foremost throughout the development process. (Learn more in "Standard," page 4.)

Public interest groups will continue to pressure retailers, manufacturers, developers and government to protect consumers' data, but the digital marketplace will remain a challenge to tame. ■

Stand up for data privacy!

Use Consumer Action's free Take Action! Center (*bit.ly/email-Congress*) to email your elected officials.

Will EU rules boost U.S. data privacy rights?

By Ruth Susswein

American consumers, particularly millennials, have a growing unspoken arrangement with some corporations, where we pay for services with our personal data. We may, even unknowingly, trade our online preferences, location data or other personal information for free access to products and services such as social media apps and networks.

When strong data protection rules take effect in Europe this May, consumers worldwide might see some ripple effect that could benefit us all. Why? The new General Data Protection Regulation (GDPR) applies to any company or organization that operates in the European Union (EU) or sells goods or services to customers in Europe. Major corporations are unlikely to create multiple, distinct and conflicting systems to handle individuals' data protection, retention, correction and deletion rights, which means new rules should apply to all customers of global corporations.

There are already signs that consumers outside the EU might benefit when U.S.-based corporations update their terms to better explain and protect the use of personal data. Even though firms are under no obligation to follow the new EU rules in the U.S., some companies have been busy doing "data hygiene"—cleaning up their data collection and retention practices in preparation for the new overseas rules. U.S. companies appear to be asking: How much data do we really need?

However, since Americans have no national data protection law to rely on, we should not expect corporations to fully comply with the new EU rules within the U.S. (For details, see "New data protection rights," page 1.)

Minimizing use/reuse

Big corporations are evaluating how to reduce the amount of data they gather and store to comply with the new rules' data minimization standards. This principle requires firms to use only as much personal information as is needed to complete a task. That means that companies must consider if the data they're collecting is relevant, useful and necessary to retain. Data minimization also demands that data collected for one purpose not be used for another purpose without consumer consent. This is a basic principle long touted by privacy advocates.

Global companies like Microsoft, Apple and Google, as well as many others, must consider data collection and protection as they design their next generation of products. Mindful of the upcoming EU directives, some companies are giving all customers more control over how their personal information is used and distributed. Google has begun letting consumers choose the data points they want to share via Gmail, and Facebook has unveiled a new data privacy center designed to let users set parameters on who may access their posts (http://nyti.ms/2EHDwgf).

Data breaches

Under an assortment of state laws in the U.S., companies are obligated to notify consumers of a data breach involving personal information. (Alabama and South Dakota are exceptions.)

Come May, companies operating in the EU will be required to report data breaches quickly to EU data protection authorities—within 72 hours of a breach—and, in high-risk cases, to report it directly to the consumer, too. While this seems like a commonsense approach, it wasn't the norm. Uber, for example, hid a major breach from the public for almost a year.

The EU breach notification requirements may prove helpful to a company's customers worldwide. Had the 145 million Americans affected by the Equifax data breach been notified months sooner, people might have taken steps to secure their data more quickly (for example, by placing a security freeze on their credit files) and reduce the risk of fraud.

Homegrown protection

Right now, protection of U.S. consumer personal data focuses primarily on notice, and, in some cases, on principles of consent and harm.

Consent: While Americans have no comprehensive data protection law, U.S. consumers do have certain protections depending on the type of data collected. For example, under the Health Insurance Portability and Accountability Act (HIPAA), medical providers, pharmacies and insurers must disclose how an individual's data will be used and generally list the entities it may be shared with for treatment or billing purposes. Healthcare providers must get written consent to allow others access to consumers' protected health information. Consumers must "authorize" (a stricter standard) the use of their health data for other purposes, like marketing or sales.

There are other federal laws that protect health information in school records, genetic data and substance abuse records. For details on these, see the Privacy Rights Clearinghouse's health privacy information page (http://bit.ly/2sOJLh9).

Under the federal Fair Credit Reporting Act (FCRA), access to some of the financial information in our credit reports is not allowed without our consent unless the company accessing it has a "permissible purpose" to obtain it. For example, credit card companies that offer you an actual credit line (not just an invitation to apply) are allowed access to your credit report without your prior agreement.

For online data, the Federal Communications Commission (FCC) had issued an internet privacy rule requiring internet service providers (ISPs) to obtain users' permission before sharing their personal information (including browsing history) with others. But that online privacy rule was repealed early in the Trump administration.

The Children's Online Privacy Protection Act (COPPA) protects any information collected or used online, or by an app, that can identify children under the age of 13. It requires parental consent before collecting children's personally identifiable data. This federal law also gives parents the right to review or delete their children's data. Personal information that is collected must follow the data minimization principle of keeping data only as long as necessary to provide a desired service. For more information, see the "Complying with COPPA" webpage (http://bit.ly/2oe4bet) by the Federal Trade Commission (FTC).

Notice: The Gramm-Leach-Bliley Act requires financial firms (lenders, insurers and investment companies) to disclose their information sharing policies, explain how they safeguard customers' sensitive data, and reveal how consumers can opt-out of having their personal data shared with other companies.

Many companies doing business in the U.S. have privacy policies posted on their websites, often with unintelligible language explaining what they will or won't do with our personal information. However, companies that do business with California consumers online or by mobile app must comply with the California Online Privacy Protection Act (CalOPPA).

CalOPPA requires companies that collect any personally identifiable information (home or email address, geolocation, etc.) from California consumers to disclose:

- What type of data is collected online or by mobile apps,
- Any third parties the data may be shared with (for example, a billing or marketing company),
- Whether third parties may access your personal data from this company,
- How consumers can change or delete their personal data,
- How the company deals with Do Not Track requests, and
- A conspicuous link to the company's privacy policy.

The patchwork of U.S. privacy protections helps to limit access to some identifiable financial or medical data, but too often companies collect personal information about us without our knowledge or consent. These firms may draw conclusions that can affect our access to jobs, credit, housing and more.

The Federal Trade Commission uses its authority to combat "unfair and deceptive practices" to protect our privacy and personal data. This agency is responsible for ensuring compliance with U.S. data privacy laws, including the Fair Credit Reporting Act and the Children's Online Privacy Protection Act.

But, in reality, the FTC has very limited authority. It can only sue a company after harm has been done, and it has limited ability to fine data violators. The agency can and does raise privacy concerns, but does not have the legal authority to write rules to help protect our data.

With no effective data gatekeepers in the U.S., consumer advocates have been heightening the call for a U.S. independent data protection authority, and for comprehensive individual privacy rights to better protect our personal information. Several states are stepping in to fill the void with new statewide privacy protections. Unfortunately, deep-pocketed corporations and other special interests have managed to block some of them.

As consumers become more aware of their limited ability to control their personal information stored in corporate databases, the EU's new data protections may help draw attention to the need for better data protection here at home. ■

Californians aim to take data privacy to the ballot box

Organizers of the California Consumer Privacy Act ballot initiative hope to put it before state voters this November (2018). Specifically, the initiative, if passed, would:

- Require businesses to protect consumers' personal information and hold businesses accountable if one's personal information is compromised by a data breach;
- Give consumers the right to know what personal data is being collected about them and when their information is bought and sold;
- Allow consumers to prevent corporations from selling private data about them to third parties; and
- Protect consumers from being discriminated against by businesses that collect consumer data and use it for decision making.

For more about the initiative, visit the CAPrivacy.org website (https://www.caprivacy.org).

Standard for measuring data privacy, security

By Monica Steinisch

The popular magazine *Consumer Reports* has published the results of product quality tests, on everything from air conditioners to yogurt, for decades.

Consumers have consulted the reviews millions of times as part of their pre-purchase research process. While Consumer Reports' mission hasn't changed, the marketplace has.

From Fitbits to smart appliances, consumers are always "connected" these days, leaving us susceptible to data breaches and identity theft. To help us protect our data, Consumer Reports advises consumers to use strong and varied passwords, and two-factor authentication, which requires users to supply a second form of ID to access an account (http://bit.ly/2HyYnEC).

The group has also called on companies to improve their data protection practices. Consumer Reports' "Digital Standard" provides guidelines aimed at influencing how internet-connected products are designed so that consumers' data security and privacy are a priority in the product development process.

The standard will help Consumer Reports and other testers evaluate "smart" TVs, health-and-fitness apps, baby monitors, thermostats, cars and other connected products based on how well they protect consumer privacy and security.

Ratings based on this new gauge are meant to empower shoppers to make informed buying decisions, and encourage companies to up their data security and privacy game to outdo the competition.

The standard calls upon companies to:

- Build products that are more secure and tougher to hack;
- Require consumers to create a unique username and password (when connecting devices to home Wi-Fi);
- Delete consumer data from their servers upon request (or account closure);
- Protect personal data with encryption when the information is transferred over the internet;
- Continually update their software with security patches as new kinds of malware emerge;
- Be transparent about how personal consumer information is shared with other companies and give consumers a reasonable amount of control over their data; and
- Notify the public quickly after a security breach.

On Feb. 7, Consumer Reports released evaluations of smart TVs and streaming video players based on the new standard. It found that some of the biggest smart TV brands are vulnerable to hackers.

Testers were even able to remotely control one TV set via the web. While researchers found that smart TVs did ask permission to collect viewing and other data, "it wasn't always clear what you're agreeing to," and if you limited data collection, you also limited the TV's functionality (http://bit.ly/2GxKRjf).

The organization will be discussing its new digital standard at, among other events, PrivacyCon, the FTC's annual privacy conference, a public event held in Washington, DC.

Developed in partnership with leading privacy, security and consumer rights organizations (https://www.thedigitalstandard.org/), the guidelines are a direct attempt to address the vulnerability of consumer data, as evidenced by the staggeringly large numbers of consumers affected by major data breaches in 2017 alone.

"While the pace of new technologies is exciting and brings greater convenience to our lives, it also carries with it new threats to our security and personal privacy," said Marta Tellado, president and CEO of Consumer Reports. "We want to ensure that consumers remain in the driver's seat when it comes to the safety and security of their personal data."

Researchers, developers, advocates and hobbyists who want to help shape the evolving guidelines are invited to provide feedback and propose changes to the open-source project (https://www.thedigitalstandard.org/the-standard). ■

Jan Philipp Albrecht, a member of the European Parliament, proposed the European Union's General Data Protection Regulation in 2013 and is often called the "father of the GDPR." (Photo: Stephan Röhl)

Europeans

Continued from page 1

when the data is no longer needed for its original purpose or consent is withdrawn. There are additional requirements if this is a child's data. Data that is inaccurate or processed illegally is required to be deleted. However, the right to delete is not absolute. In some cases consumers can only limit the use of the data.

Right to limit data processing: Consumers can block personal data from being processed if the data is disputed as inaccurate. The disputed data can be stored, but not used until the dispute is resolved.

Right to object: Consumers will have the right to object to having their personal data used for direct marketing or profiling purposes.

Right to avoid automated decision making: Consumers can choose not to participate in decisions that are exclusively computer-driven if the decision could harm them (such as hurt their credit record if they were denied credit).

Right to data portability: Consumers have the right to receive a copy of their personal data, and can transfer the data to another provider. This only applies to data that a consumer provides to a company.

Consent

A consumer who requests or uses a service (opens a bank account, for example) is considered to be providing consent to share her data with the company that supplies the specific product or service. Under the GDPR, consumer consent must be "freely given, specific, informed and unambiguous." The company providing the service is considered to have a "legitimate interest" in the data.

For the collection, processing and use of personal data for any other purpose than its original use, companies must seek consumers' consent via "a statement or a clear affirmative action" (for example, a checked box). The GDPR states that "silence, preticked boxes or inactivity should not … constitute consent." Consumers have the right to withdraw consent at any time.

For access to or use of consumers' most sensitive information (for example, health or genetic data), companies are required to get consumers' explicit consent to use the data for a specific purpose other than what the data was collected for. Explicit consent means a consumer clearly chooses to agree to the use of their personal information. It may be written or oral.

Recourse

Companies with more than 250 employees will be required to include privacy protections in all their business practices. Companies that regularly process sensitive data must have a data protection officer on staff. "Controllers" and "processors" of personal data will be responsible for following the new rules, but companies considered data controllers would have the primary responsibility. Controllers are defined as those firms that decide how data will be used, and processors process, collect, record and maintain data for controllers.

If data protection rules are not followed, consumers can file a complaint with the EU data protection authority in that state and seek compensation for the harm.

Companies that do not comply with the new GDPR rules could be hit with huge fines, totaling four percent of their global revenue. While these data protection rules only officially apply to citizens in the EU, they may well impact consumers worldwide, as major corporations that want to avoid the risk of millions in fines may invest in standards that protect customers no matter where they live. ■