FEATURE STORY

RILA On How United States Retailers Are Responding To **Changing Privacy Rules**

– *Page 8*

NEWS & TRENDS

U.S. senator proposes federal agency to target online information security, big technology firms – *Page 12*

DEEP DIVE

Examining U.S. open banking regulatory confusion and its merchant impacts – *Page 18*

Merchants Guide To Navigating

GLOBAL PAYMENTS REGULATIONS

PYMNTS.com | EKATA

MARCH 2020

Merchants Guide To Navigating

GLOBAL PAYMENTS REGULATIONS

PYMNTS.com | EKATA

TABLE OF CONTENTS

ACKNOWLEDGMENT

The Merchants Guide To Navigating Global Payments Regulations was done in collaboration with Ekata, and PYMNTS is grateful for the company's support and insight. PYMNTS.com retains full editorial control over the following findings, methodology and data analysis.

WHAT'S INSIDE

The European Union is still the blueprint for regulators looking to launch online data transactions and payment rules thanks to its General Data Protection Regulation (GDPR) and revised Payment Services Directive (PSD2), which the European Commission passed in 2018. These two rules are guiding new laws in other regions, with notable shifts in data transparency and privacy taking place in Australia, China and the United States, for example.

Agreeing on these rules can be tricky, especially in the U.S., where both state and federal governments can dictate regulations. The country is experiencing many developments in online data privacy and security, with several states issuing consumer protection laws. Each is proposing rules with varying levels of strictness and transparency, however, making universal adherence difficult if not impossible. Washington State, for example, is specifically targeting big firms that collect data, like Facebook and Google, with the Washington Privacy Act (WPA). California has a more sweeping law, the California Consumer Privacy Act (CCPA), which passed in January and is causing concern among businesses, consumers and lawmakers regarding where and how it applies.

The country's view on data and open banking is fractured and regulators are debating these laws' full scopes, creating both challenges and opportunities for players that want to participate in the U.S. economy. Open banking developments are occurring worldwide, too, with regulators in Australia and the EU examining additional changes in their markets. The new coronavirus has made it harder for legislators to plan regulatory decisions, with COVID-19's advancement forcing many businesses, banks and consumers to take their work and spending indoors

and online. The financial industry was among those that needed to make large-scale changes and is currently struggling to recover after adapting to remote operations. How consumers and merchants react to such disruptions could have major impacts on how open banking is treated in the future.

AROUND THE DATA PROTECTION WORLD

COVID-19's impact comes during a time of change for many regulators, including those in the U.S. government that are debating how firms should treat data. U.S. lawmakers are looking at new ways to shift open banking and privacy standards, with Sen. Kirsten Gillibrand (D-NY) proposing the creation of an agency that would directly deal with consumer complaints regarding firms that are mistreating information. The agency would regulate how larger technology companies, such as Facebook and Google, could use, share or monetize data within the U.S., and work with existing committees to ensure compliance among those under its jurisdiction.

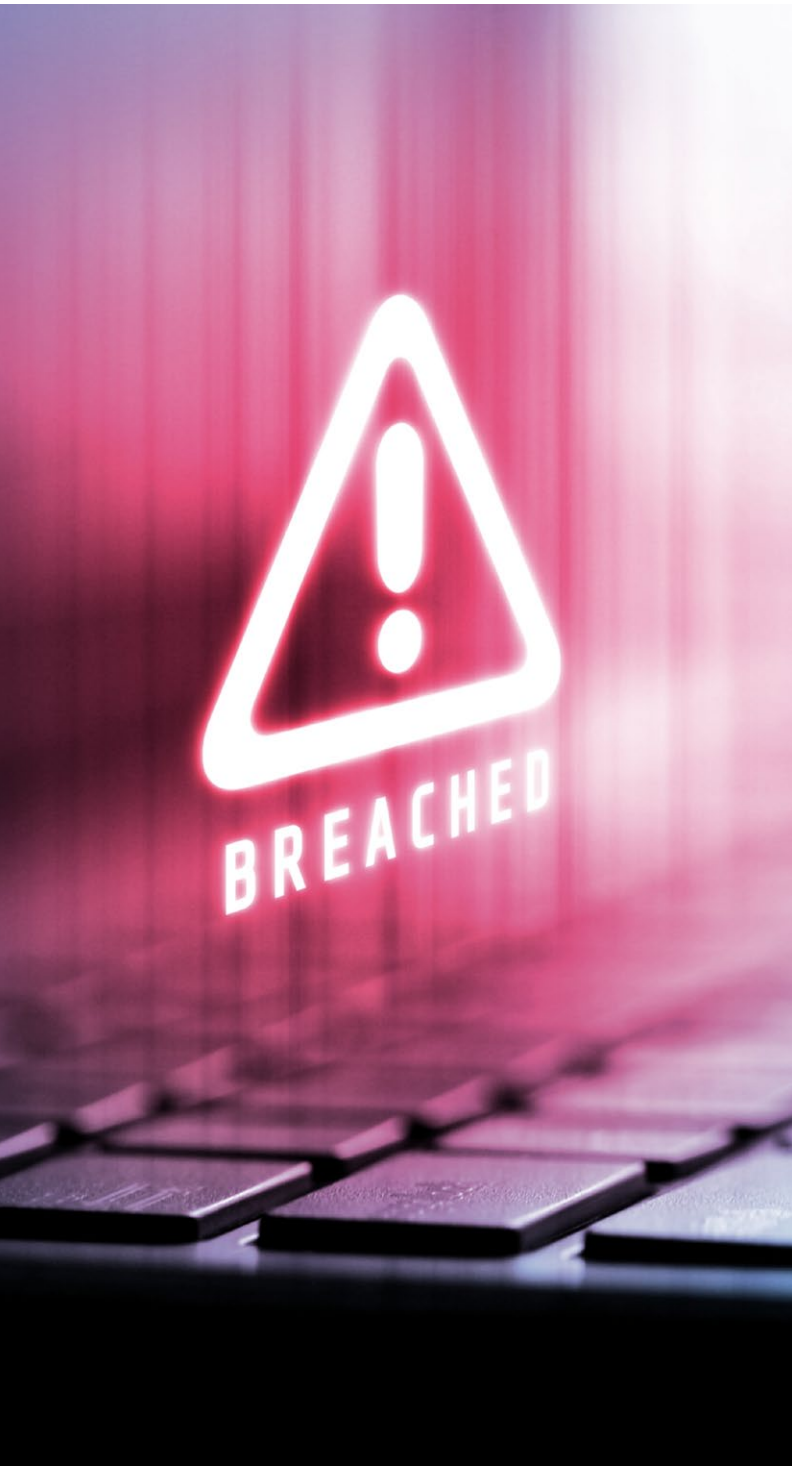
Banks, merchants and payment providers in the EU are also rehashing familiar conversations, once again debating how GDPR, which limits the collection of healthcare data, may be enforced during the pandemic. These provisions are relaxed during emergencies but not entirely removed, leading to confusion about which data can be safely collected. Merchants are thus turning to their payment and bank partners for answers on how GDPR's emergency rules will apply to their operations.

Other markets made broad changes to their financial industries just before the COVID-19 outbreak, forcing many to regroup with remote work and online transactions. Businesses and banks are juggling this online focus with open banking regulations that have only just been passed. The Australian Competition and Consumer Commission (ACCC) recently publicly released guidelines for open banking in the country following details outlined in its 2017 Consumer Data Right (CDR) provision, for example. The CDR outlines which data banks and other financial entities must share with consumers and aims to create transparency and security for all parties. Banks have until July 1 to innovate their infrastructures and comply with the new standards, giving them some leeway as they figure out how to operate digitally in the era of COVID-19.

For more on these stories and other global data and payment regulations headlines, check out the Tracker's News and Trends section (p. 12).

RILA DESCRIBES HOW NEW RULES ARE AFFECTING US SECURITY

California, New Jersey, New York, Washington and other states are all developing or implementing regulations meant to deal with online data security and payments. Merchants must take the necessary steps to remain compliant with these new rules, but their prime directives remain the same: They must



create experiences that satisfy their consumers, regardless of the privacy laws under which they fall. Crafting such experiences requires that they have access to the data under discussion, however. For this month's Feature Story (p. 8), PYMNTS spoke with Nicholas Ahrens, vice president of innovation at U.S. retailer trade group Retail Industry Leaders Association (RILA), to find out how merchants are responding to changing data rules while keeping their grasp on the details they need to stay competitive.

DEEP DIVE: US OPEN BANKING FRAGMENTATION AND ITS IMPACT ON MERCHANTS

Sixty-three percent of U.S. merchants reported that they suffered at least one data breach that compromised a minimum of 1,000 sensitive records in 2019. There is an obvious need to upgrade rules and protect information from fraudsters, but relevant parties must be able to easily access these details to provide personalized customer experiences. Multiple states are drafting privacy laws with these restrictions in mind, and these rules are in varying stages of discussion, with some regulators changing and upgrading them even after they become effective. This month's Deep Dive (p. 19) examines privacy complexities in the U.S., how fragmentation is frustrating merchants and how the privacy world will evolve.

5 FIVE FAST FACTS

$62.4B

Value of revenue affected by new SCA-based contactless card regulations in the EU

28%

Portion of consumers with clear understandings of which data points companies can keep under GDPR

20%

Share of consumers who stated they understood what the term "open banking" meant

33.3%

Portion of businesses that claimed to understand GDPR requirements

63%

Share of U.S. businesses that reported experiencing a data breach that compromised at least 1,000 records in 2019

RILA ON HOW UNITED STATES RETAILERS ARE RESPONDING TO

CHANGING PRIVACY RULES

FEATURE STORY

CCPA, WPA and other new privacy and online transaction standards are changing how businesses interact with consumers' data in the U.S. Retailers are dutifully speaking with their payment service providers (PSPs) and industry partners to adhere to these shifts, but they must also keep their customers' experiences in mind. Personalized experiences require merchants to have access to data — a crucial resource in helping them distinguish themselves from competitors.

The nation's ongoing debate about privacy is similar to that which took place in the EU prior to PSD2's and GDPR's introductions. U.S. states are starting to implement new standards, too, with the CCPA introduced two months ago and WPA on the path to ratification in Washington. The critical question, then, is not whether retailers can comply with these rules, but how they will do so while remaining competitive, Nicholas Ahrens, vice president of innovation at U.S. retailer trade group RILA, told PYMNTS in a recent interview.

"There is a core element of the retail business that is unchanged, which is [that] their Number One objective is to serve customers and to make sure that customers have the best possible experiences on whatever platforms [with which] they're engaging," Ahrens said. "Modern retail is not just a physical store thing or a mobile thing or an online thing. It is all of those things connected and integrated, and it is data that enables all of that to happen."

Merchants must make sure their customers' experiences match those belonging to international retailers as well as local brands, he continued. That means they must determine which data is available to them and how it can be used to cultivate

relationships with consumers wary of sharing personal details.

RETAILERS AND DATA'S ROLE

Data is being sent at an unprecedented rate — one of the main reasons there are so many rules surrounding its flow between merchants, businesses and consumers. This inundation of laws is creating uncertainty among merchants who want to keep their processes compliant, however.

Privacy conversations are old hat for retailers, Ahrens noted. Questions on how to keep data secure are expected, but those regarding usage transparency or which elements they can access are somewhat new.

"We maintain a privacy leaders council with the heads of privacy as well as payments communities, [and] this is never a new conversation," he said. "This is an ongoing conversation, so I think that as different states put out different proposals, we can continue to bring [other elements] in. But, these [proposals] are not plucked from the ether. … These are proposals that [come from] things we know and have seen and have also had conversations about."

Retailers rely on access to online buying, browsing and purchasing habits to market their goods or services and personalize existing customers' experiences. Most of the rules that state governments are discussing concern how to manage such data as information and as a critical resource. These approaches differ from state to state, but retailers' priority — enabling competitive experiences — remains the same regardless of how robust privacy laws may be, Ahrens explained. Merchants must hang onto consumers' trust, which can be difficult when data rules rapidly develop.

"[Retailers] know retaining consumer trust is vital," Ahrens said. "Every interaction is increasingly important because you are not just appearing as a retailer interacting with the market [or] just competing against fellow retailers. You are [also] competing against all the customer experiences that your customer is having. So, whether it is their engagement with [a major streaming provider] or otherwise, they are comparing the customer experience they've had with you against those [companies]."

Retailers also typically have more personal relationships with consumers as they deal more directly with them than regulators. Merchants are the first to bear the financial and other consequences when consumers are dissatisfied, and customers expect seamless experiences no matter how well-versed they are in the intricacies of open banking and security standards.

CONSUMERS AND PRIVACY CHANGES

More consumers may also expect greater access to their information in the wake of sweeping changes like GDPR and PSD2. This may be due more to the security threats they face when conducting conversations and business online, however.

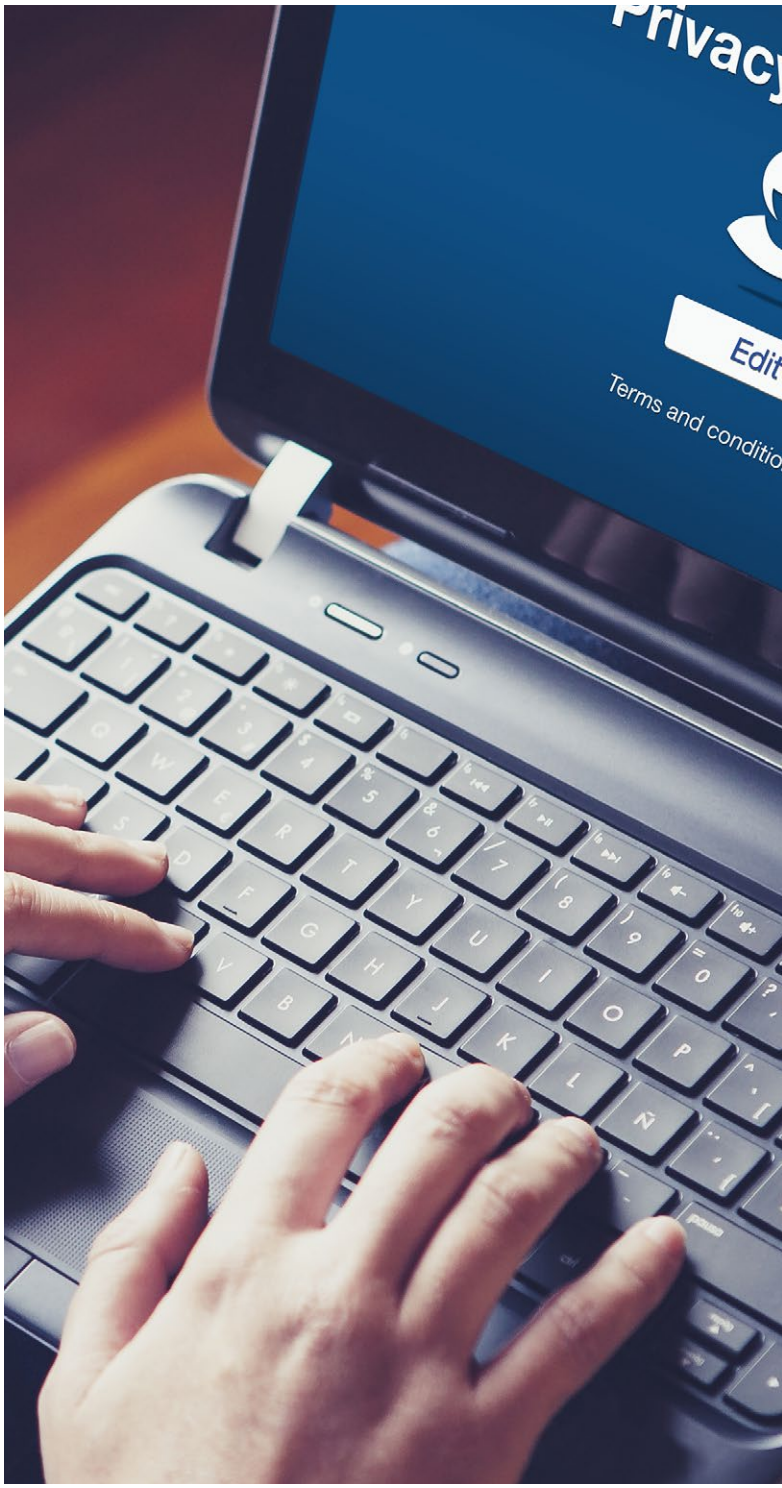
"What I do think is changing are consumer attitudes, generally," Ahrens said. "I actually do not think it is because of the law. I think it is because of broader

[consumer] awareness about the technological landscape, and so whether that is from [social media or analytics companies] or other interactions that folks have, I think people are just so much more conversive about technology. It is more of [their] daily life … and I think that, for many retailers, it changes [their] consumer interactions."

Rising consumer sensitivity to which companies hold their data and why is familiar to retailers, but the conversation carries somewhat higher stakes in the U.S. The country's standards are lacking compared to other markets in which local citizens already enjoy protections, such as the EU.

"In the broader privacy landscape, I think, obviously, Europe is the pacesetter for the world in this space," Ahrens said. "There was a time when the U.S. and Europe were both trendsetters of the privacy landscape [but], very clearly, it has swung in the direction of Europe. When you look at Brazil and other countries [that] are looking for data privacy regimes, they are emulating [those seen in the EU]."

It is unclear how many privacy rules state regulators are looking to implement, but what retailers and consumers want from these rules — increasingly transparent data access and control — stands out. Merchants will thus need to work with regulators to ensure both groups' interests remain protected.



NEWS & TRENDS

COVID-19 AND REGULATORY CONCERNS

COVID-19 FURTHER COMPLICATES GDPR

The open banking universe was not immune to COVID-19's impacts. The virus proved to be yet another test for GDPR in the EU, with businesses, healthcare services and insurers questioning how the regulation would be applicable during the pandemic. GDPR has stipulations concerning the ways businesses may collect or deal with healthcare data, similar to its restrictions on how firms handle other personal information. Companies are charged fines for noncompliance, but healthcare data's restrictions are lifted during emergency situations, which can be confusing for merchants.

The emergency rules are covered under GDPR's Article 9 and state that the blocks on processing medical information are relaxed during matters of public health. Just how relaxed is up to EU regulators, however, and will likely remain a point of contention as firms search for clarity on which information can be processed under Article 9.

WHO ADVISES USE OF DIGITAL PAYMENTS

COVID-19 may also have long-term impacts on the financial industry, as consumers and merchants adapt their payment methods to minimize contamination. The World Health Organization (WHO) issued a statement advising consumers to choose alternative payment methods, such as contactless payments, that could prevent the spread of the virus. This would mean avoiding payments made with cash, which changes hands often during payment. The Bank of Ireland has responded to this request by waiving its contactless fees for consumers to encourage use.

Contactless payments are governed under PSD2 in the EU, and such moves could lead to greater adoption of the method in the future. It could also further reduce cash usage among consumers in multiple markets, especially if merchants ban cash use in their physical stores.

US DATA TRENDS

US SENATOR PROPOSES NEW AGENCY FOR DATA PROTECTION

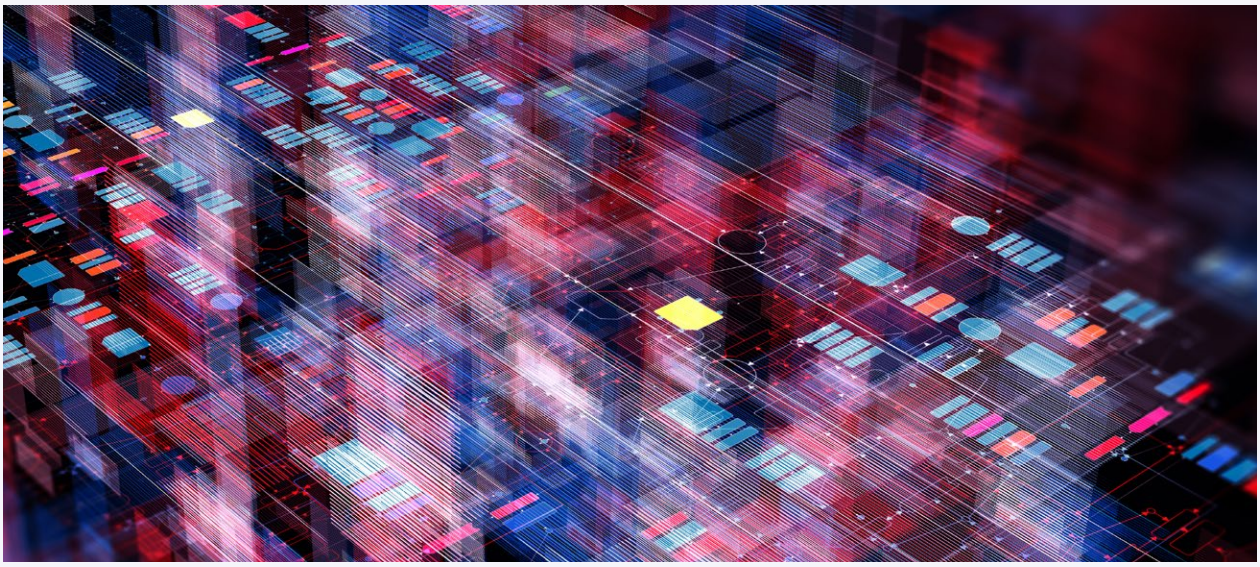
The shuttering of businesses and major financial processes in COVID-19's wake follows major developments in open banking laws for countries like Australia and the U.S. Lawmakers at all levels in the U.S. have been debating how data should be treated or protected for several months, with a recent strategy coming from Sen. Kirsten Gillibrand (D-NY). Her proposal outlines the creation of a dedicated federal agency that would handle consumers' data protection. The proposed Data Protection Agency (DPA) would address consumers' complaints about firms misusing their personal information, according to Gillibrand's outline. Companies found in violation of federal data privacy rules could then be disciplined in various ways, including with civil fines.

The senator's plan mentioned Google and Facebook as examples of companies that the agency would regulate, and the DPA would also work with existing committees and state agencies to keep consumers' data safe. It is not yet clear if such a department would eventually be created to handle online privacy in the U.S.

CALIFORNIA LAWMAKERS DEBATE CCPA UPGRADES

One of the most recently discussed privacy regulations is the CCPA, which went live in California at the beginning of this year. The state's attorney general is already proposing upgrades to the rule after only two months of active status. Businesses and consumers are expressing concerns regarding the law, and proposed changes include how to approach consumers' opt-out options, which are often translated into website buttons that customers can click to be removed from collection processes. These opt-out buttons must be transparent and easy to find, according to the attorney general.

Other changes address concerns about what is considered personal information. The central question surrounds whether these details are data that can be directly linked to individual consumers, such as their home addresses or Social Security numbers, or whether it includes information like IP addresses, which may be more easily divided from individuals' core identities. The state has yet to enact the upgrades, and regulators will likely continue to debate them for several months while they collect more opinions from businesses and consumers.



NEW JERSEY CONSIDERS STATE DATA PRIVACY RULE

New Jersey is following California's lead, with the state's legislators crafting a bill that uses both the CCPA and the EU's open banking and privacy regulations as blueprints. The bill would apply to information collection and usage standards for larger technology companies operating in New Jersey and would require these companies to get explicit permission to collect personal information from residents. New Jersey lawmakers held a public hearing on the issue on March 16 to address related concerns and opinions.

The potential rule would mandate that companies outline how the data will be used when asking for permission to collect it. This goes a step beyond other U.S. regulations, including California's, which require only that companies obtain consumers' consent before utilizing their information. Those firms are not yet required to explain where or how they will use that data when customers opt-in to cookies or other forms of data collection.

WA FLESHES OUT STATE PRIVACY ACT

CCPA, GDPR and PSD2 were also used as blueprints for Washington State's open banking and online data law. State legislators proposed three consumer transparency bills in January, the WPA among them. The bill was introduced one year after its draft failed to pass, though its details are still being debated among state officials and concern data collection

among private companies. The latest version of the WPA passed into the Washington Senate on Feb. 18, with the state's House offering amendments a few days later. State lawmakers are presently examining two different versions of the same privacy act.

The WPA is unique among other U.S. data privacy rules in that it specifically focuses on larger companies, applying only to firms that receive 50 percent or more of their revenues from the sale of personal data or those that process data belonging to 100,000 or more individual consumers during one calendar year. One proposed amendment lowers the revenue threshold to 25 percent.

US BANKS, FINTECHS JOSTLE FOR CONTROL OVER CONSUMER DATA

Banks and smaller FinTechs in the U.S. are both aiming to be chosen to access and protect data, with each side arguing its benefits for companies. Banks state that data is less secure in FinTechs' hands, while FinTechs argue that removing their access to data will hinder them from competing with more established financial players. This is an old debate in the financial space, but deciding which companies have access to what data and why is becoming more important as consumers look for more transparency into how their personal information is being used.

J.P. Morgan is exploring one potential solution while also finalizing deals with several data aggregators — companies that collect information and distribute it to FinTechs — for more strident standards. It has already signed an agreement with software company Yodlee, restricting which data the latter can access or share with financial applications. Other aggregators are not pleased with this solution, however, and have asked the Consumer Financial Protection Bureau (CFPB) to supervise data collection for more security. This would allow them to collect more data and stay competitive while keeping consumers' personal details secure.

GLOBAL TRENDS AND DEVELOPMENTS

EU UPGRADES PLANS FOR INDUSTRIAL DATA SECURITY, PRIVACY

European regulators are keeping a close eye on changing data developments in other countries, including China and the U.S. The European Commission is looking to consolidate approaches to industrial data similarly to how it coordinated banking rules under PSD2, according to recent reports. This would prevent EU companies from having to outsource to other firms for certain types of data and help them approach data use among large-scale companies, including Amazon, Facebook and Google.

The prior consolidation under PSD2 saw the EU upgrade the way banking data was shared from established banks to third-party players such as FinTechs, opening the flow of information to more

entities. The commission's new plan for industrial data could force the EU to levy more taxes on companies that are not native European firms, but it is still outlining the details and how the proposal could affect businesses within its borders as well as those that rely on EU data.

ACCC RELEASES OPEN BANKING REGULATIONS

The EU's impact on other markets is expanding, with Australia's ACCC officially releasing open banking rules for banks and FinTechs under CDR, which gives individuals rights similar to those detailed under GDPR. CDR allows Australian consumers to view data held by Australian businesses and request that banks share their information with accredited third parties. Banks are required to begin sharing data with consumers by July 1, although they have extended time to prepare more complex data packages. Details on mortgages and personal loans do not need to be shared until Nov. 1, for example.

SCA CONCERNS RESURGE

UK MERCHANTS SCRAMBLE TO MEET SCA COMPLIANCE

Merchants and banks were given ample time to comply with strong customer authentication (SCA), with the deadline for doing so passing in the United Kingdom on March 14 — six months after the original policy deadline. Market players were still questioning SCA's potential implications earlier this month as the deadline crept up, and some U.K. firms had additional worries thanks to Brexit, which prompted law changes that have yet to be fully defined but could mean possible changes for banking and payments in the country. Third parties and PSPs were all required to meet SCA compliance by the March deadline, however, regardless of lingering confusion.

Payment providers are exploring both behavioral and biometric identifiers to comply with SCA, which mandates two-factor authentication (2FA) for online transactions. Firms can choose to apply combinations of knowledge-based questions like passwords and more secure options such as fingerprints or voiceprints. Merchants can utilize any combination of these factors as long as their payment partners support them.

SCA CAUSES CONTACTLESS PAYMENT STRUGGLES

Merchants across the EU have become more comfortable with PSD2's and SCA's compliance requirements, but the same cannot be said of consumers. SCA's mandated authentication measures could lead to approximately €57 billion ($60.9 billion USD) in abandoned transactions from customers who do not want to deal with the extra identification checks associated with contactless and digital payments, according to one report. A separate report puts the revenue lost for these businesses at about

$62.4 billion. Contactless payments are growing more popular in Europe and throughout the U.K., but SCA requires consumers' identities to be verified each time they hit certain purchase limits. These measures may require shoppers to input their PINs or other identifiers into websites or physical point-of-sale (POS) systems, though some simply choose to instead abandon the transactions. Customers are already likely to abandon purchases even without SCA's added frictions, with one report finding that 69 percent of purchases were abandoned in 2019. Twenty-seven percent of those who did so stated it was because of complicated checkout processes. Adding in additional authentication measures is unlikely to simplify them for consumers.

GDPR AND PRIVACY

GDPR CONCERNS AFFECT GOOGLE'S DATA STRATEGIES

Even large companies can struggle to keep pace with shifting data and privacy requirements, as evidenced by technology company Google's recent concerns regarding storing user data. The U.K.'s move to leave the EU means that Google — as well as others operating similar servers — may not be able to store U.K. users' data in the same areas in which it stores that of European users. Google is currently planning to store U.K. users' data on its U.S. servers, noting that British regulators and other authorities will still be able to access it with ease.

Questions remain over whether GDPR and similar regulations will still apply to Britons' personal data in the long term, and there are also worries about the level of access U.S. regulatory officials would have to said data if it were located within U.S. borders. These questions will likely continue to be debated as Brexit's impacts on data privacy become clearer. Consumers still have questions regarding the rule,

too, with only 28 percent of EU residents stating they understood which data companies were allowed to keep under GDPR. Another report noted that just 20 percent of consumers understood what "open banking" meant, which suggests that confusion remains regarding these rules.

FACEBOOK SLAMS INTO EU PRIVACY BARRIERS WITH DATING FEATURE

Social media service Facebook is also dealing with EU privacy laws' effects on its operations. It recently clashed with the Irish Data Protection Commission (IDPC) over plans to launch its Facebook Dating feature in the EU just before Feb. 14. The IDPC stalled the launch on claims that Facebook had not filed the proper paperwork, including the data processing impact assessment (DPIA) form required under GDPR. The company has since released a statement confirming its wish to remain compliant with GDPR and has thus postponed its Facebook Dating release in the EU.

The IDPC currently has 11 open investigations into Facebook regarding its use of data and whether it has breached the regulation. The regulator is checking Google's data use as well while also examining cases associated with technology company Apple and social media platform Twitter. These companies may simply be confused about what is required of them, however, as one survey found that just 33.3 percent of businesses fully understand GDPR's mandates.

EU ADDRESSES FACIAL RECOGNITION GDPR CONFUSION

Companies in the EU have also struggled to understand if they can collect specific data or use certain technologies under GPDR, including biometrics like fingerprints and facial scans. Margrethe Vestager, executive vice president of digital affairs for the European Commission, answered these concerns in a recent interview, noting that companies should probably avoid using automated facial recognition technology as they then risk breaching GDPR. These technologies do not allow companies to gain consumers' consent before they are applied, she clarified, adding that consent is critical to personal information's use under the regulation.

That is not to say that GDPR explicitly bans facial recognition technology, however. Its use requires informed consent from consumers, who might have their faces or other biometric data collected for companies' use. Balancing those two elements is tricky for firms, and the commission will be researching potential consequences and use cases before sending out applicable legislation, Vestager noted.

DEEP
DIVE

How US Data Regulation Fragmentation Is Affecting Merchants, Consumers

Devising open banking laws that adequately respond to shifting privacy needs and satisfy both businesses and consumers is difficult. U.S. legislators in several states are either drafting, voting on or have passed requirements to tackle online data's and transactions' importance, but these laws often do not integrate well with those passed in neighboring states. Discussions can be further complicated by world events that change the way FIs, businesses and consumers interact. The COVID-19 pandemic has led to a jump in online payments versus those made in stores, for example.

Such regulations' necessity is undeniable, however, as lagging data standards leave businesses and consumers open to fraud and boost frustrations regarding digital transactions' speeds. Sixty-three percent of U.S. businesses experienced at least one data breach that compromised a minimum of 1,000 records in 2019. Coming up with comprehensive rules regarding what data may be shared and how will provide deeper layers of protection for businesses and consumers while also allowing the former to create more personalized services and compete on a global stage.

It can be difficult for U.S. merchants to understand which data may be accessed, however, and this is becoming more challenging as state legislators change, adapt and stretch their open banking and privacy laws. California, New Jersey, New York and Washington have different laws, for example, and companies operating in all of these states must comply with each. Such complexities are frustrating for consumers, who are now confronted with messages asking them to share their details or opt out of doing so.

It is thus critical that merchants take comprehensive looks at recent shifts in U.S. data privacy laws and how companies can comply with any and all of these new rules.

DECLUTTERING THE US PRIVACY ARENA

Each state regulator is trying to answer two simple questions regarding these new developments: Which data is important, and which companies can access it? Answers to these inquiries have proved elusive, however, largely because access to privileged information has become key to how one business succeeds over its competition.

Data is valuable and merchants are caught in the middle, as evidenced by the recent questions arising in the EU regarding GDPR's applicability to healthcare data during the COVID-19 outbreak. Merchants are still unsure which data they have access to under GDPR's emergency laws, further exacerbating existing confusion over its restrictions. Similar debates have played out in other markets, including California, where merchants can respond to data barriers under both the CCPA and its Assembly Bill 5, or the "gig economy bill," regulating data that businesses and freelancers share.

Which companies should — and, most importantly to regulators, should not — have access to data underpins the laws being passed worldwide, from China's rules governing foreign entities to the battles between social media giants like Facebook and EU lawmakers. This years-long conversation has resulted in regular privacy standard changes and upgrades, but shifting goalposts present a real source of frustration for merchants. These firms are expected to comply with all new rules that present themselves, both in their home countries and abroad — a costly endeavor. U.S. companies spent more than $82 billion on compliance solutions last year, according to one report, and many experts expect these costs to increase given the questions that remain over privacy and online transaction rules.

Fragmentation in U.S. privacy standards is such that merchants can have full access to consumers' personal data in one state but may be unable to touch crucial details in another — an especially frustrating factor for merchants that conduct business online. The guidelines for data transmission state by state are equally unclear: Legislators in Washington, who are proposing the WPA, are adamant that large technology companies like Google should not have access to the personal information they currently do, for example. This represents a problem for smaller merchants as well because many rely on companies like Google or Facebook for the data they use to market to or interact with customers.

Other lawmakers are more willing to open online platforms to a broader swath of firms, but that comes with its own set of troubles. The CCPA is strict with these companies, for example, but the merchants to which the rules do apply and the consequences for noncompliance are less clear as a result. Figuring these details out can prove costly, as well: Online invitation service Evite spent $1 million attempting

to determine its privacy requirements under CCPA, according to a recent article, and that was after it stopped selling personal information to third parties. It also posted a "do not sell my info" button on its site in addition to its policy change. Other firms have followed Evite's example in the two months since CCPA became effective.

Such confusion is detrimental to merchants and concerning for the future. Many U.S. companies have watched similarly murky regulations affect businesses in Europe, where SCA measures could potentially lead to EU merchants collectively losing $60.8 billion from consumers who abandon transactions because of added payment frictions. It is difficult to generate loss predictions for U.S. merchants because the rules differ from state to state, but it can be assumed that companies may suffer similar declines in revenue and customer conversions. Defragmenting the U.S. privacy market is thus a matter of necessity for merchants, but this is easier said than done.

EXAMINING PRIVACY WORLDWIDE

U.S. regulators are searching for solutions that can make the privacy landscape more cohesive, with Sen. Kirsten Gillibrand making regulatory proposals at the federal level, but such legislation is still in states' hands. Most U.S. merchants operate online and internationally, meaning they not only need to comply with U.S. privacy laws but also those in other countries.

Developing international standards for data access and open banking could ease merchants' confusion in this area, especially as more businesses operate on a global scale. This would require a single body to agree on a full suite of rules for international application, however, which would likely take years. Many markets are using the EU's approach to open banking and privacy as guidelines, but GDPR's true reach remains unclear. Regulators have issued $126 million in fines for noncompliance since the rule's 2018 introduction, but it is worth noting that much of that figure comes from larger fines levied against companies like Google. Many smaller merchants are relying on their banking partners for GDPR compliance and have thus kept up with the rule.

Any global standard will need to take all of this into account before it can be implemented. It will also have to answer regulators' questions — which data is important and why — which will remain central inquiries at the heart of such a standard.

ABOUT

PYMNTS.com

PYMNTS.com is where the best minds and the best content meet on the web to learn about "What's Next" in payments and commerce. Our interactive platform is reinventing the way in which companies in payments share relevant information about the initiatives that shape the future of this dynamic sector and make news. Our data and analytics team includes economists, data scientists and industry analysts who work with companies to measure and quantify the innovation that is at the cutting edge of this new world.

EKATA

Ekata is an international identity data company that provides businesses with global identity verification solutions via enterprise-scale APIs and web tools to help companies identify legitimate customers, prevent fraudulent transactions, and smooth new customer creation. Ekata services customers from offices in Singapore, Budapest, Amsterdam and Seattle.

We are interested in your feedback on this report. If you have questions or comments, or if you would like to subscribe to this report, please email us at feedback@pymnts.com.

DISCLAIMER

The Merchants Guide To Navigating Global Payments Regulations may be updated periodically. While reasonable efforts are made to keep the content accurate and up-to-date, PYMNTS.COM: MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, REGARDING THE CORRECTNESS, ACCURACY, COMPLETENESS, ADEQUACY, OR RELIABILITY OF OR THE USE OF OR RESULTS THAT MAY BE GENERATED FROM THE USE OF THE INFORMATION OR THAT THE CONTENT WILL SATISFY YOUR REQUIREMENTS OR EXPECTATIONS. THE CONTENT IS PROVIDED "AS IS" AND ON AN "AS AVAILABLE" BASIS. YOU EXPRESSLY AGREE THAT YOUR USE OF THE CONTENT IS AT YOUR SOLE RISK. PYMNTS.COM SHALL HAVE NO LIABILITY FOR ANY INTERRUPTIONS IN THE CONTENT THAT IS PROVIDED AND DISCLAIMS ALL WARRANTIES WITH REGARD TO THE CONTENT, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AND TITLE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES, AND, IN SUCH CASES, THE STATED EXCLUSIONS DO NOT APPLY. PYMNTS.COM RESERVES THE RIGHT AND SHOULD NOT BE LIABLE SHOULD IT EXERCISE ITS RIGHT TO MODIFY, INTERRUPT, OR DISCONTINUE THE AVAILABILITY OF THE CONTENT OR ANY COMPONENT OF IT WITH OR WITHOUT NOTICE.

PYMNTS.COM SHALL NOT BE LIABLE FOR ANY DAMAGES WHATSOEVER, AND, IN PARTICULAR, SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, OR DAMAGES FOR LOST PROFITS, LOSS OF REVENUE, OR LOSS OF USE, ARISING OUT OF OR RELATED TO THE CONTENT, WHETHER SUCH DAMAGES ARISE IN CONTRACT, NEGLIGENCE, TORT, UNDER STATUTE, IN EQUITY, AT LAW, OR OTHERWISE, EVEN IF PYMNTS.COM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW FOR THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, AND IN SUCH CASES SOME OF THE ABOVE LIMITATIONS DO NOT APPLY. THE ABOVE DISCLAIMERS AND LIMITATIONS ARE PROVIDED BY PYMNTS.COM AND ITS PARENTS, AFFILIATED AND RELATED COMPANIES, CONTRACTORS, AND SPONSORS, AND EACH OF ITS RESPECTIVE DIRECTORS, OFFICERS, MEMBERS, EMPLOYEES, AGENTS, CONTENT COMPONENT PROVIDERS, LICENSORS, AND ADVISERS.