WILSON SONSINI

The Data Advisor

Winter 2020

We are thrilled to provide you with the Winter 2020 edition of the Wilson Sonsini *Data Advisor*. 2019 was a remarkable year in the world of privacy and cybersecurity: EU Data Protection Authorities started enforcing the GDPR; California enacted the first comprehensive privacy law in the U.S.; and the Federal Trade Commission announced a $5 billion settlement with Facebook. We expect 2020 to be as busy and newsworthy as 2019. We will be covering these developments in quarterly issues of the Wilson Sonsini *Data Advisor*.

Please visit www.wsgrdataadvisor.com for the latest news and an archive of past articles. Our website makes it easy to browse and search all of our articles and provides a venue for us to cover emerging developments between issues.

In This Issue

FTC Trends and Forecasts: Notable Areas of Interest in 2019 and What's Ahead in 2020

By Libby Weingarten and Kelly Singleton

2019 was a momentous year for the Federal Trade Commission (FTC). Among other things, the agency obtained multiple record-breaking settlements, held comprehensive hearings on consumer privacy, and examined its longstanding practices with regard to data security and children's privacy. We expect to see similar trends in 2020, as the FTC flexes its enforcement muscles amid a growing cry for increased privacy protections and meaningful legislation.

The FTC hearings and workshops in 2019 signal new approaches to enforcement and policy priorities that we are likely to see in 2020. Most notably, the FTC held a series of hearings to examine whether changes in the economy, new technologies, and international developments require adjustments to consumer protection law, enforcement priorities, and policy. The issues addressed at these hearings included, among other things, privacy and big data, algorithms, artificial intelligence (AI), and predictive analytics, and the FTC's approach to consumer privacy and data security. Companies should look out for reports on these issues, which may contain guidance that will be top of mind for the Commission in 2020.

This article outlines the privacy, data security, and consumer protection issues the FTC focused on in 2019, what will likely be top of mind in 2020, and practical takeaways for companies to keep in mind when navigating the complex world of privacy, data security, and consumer protection more generally.

Privacy

The FTC's privacy docket was dominated by three top issues in 2019: Privacy Shield, children's privacy, and the Facebook settlement—a case so significant that it deserves its own mention.

Continued on page 2...

FTC Trends and Forecasts . . . *(Continued from page 1)*

Privacy Shield. Privacy Shield is a voluntary certification program that allows participating companies to transfer personal data from the EU or Switzerland to the U.S. in accordance with EU and Swiss data protection laws. The FTC is entitled to bring Privacy Shield cases against companies when they falsely claim they are Privacy Shield certified or fail to comply with the substantive Privacy Shield principles. The FTC ramped up its Privacy Shield enforcement in 2019, settling cases against more than half a dozen companies, and will likely continue to do so in 2020. This should come as no surprise after the European Commission called on FTC to "further step up" its Privacy Shield investigations in late 2019.[1]

Key Takeaways:

- Complete your certification before representing that you participate in Privacy Shield. The FTC has brought cases against companies for stating in a privacy policy or other public statements that they participated in Privacy Shield before they completed the application process. Companies should make sure that they have completed the application and have been certified by the Department of Commerce before they make any representations about Privacy Shield participation or certification.

- Remember to recertify annually. If a company lets its certification lapse, it will be removed from the Privacy Shield list and can no longer claim that it participates in Privacy Shield. The FTC has brought cases against companies that continue to make these claims after letting their certification lapse. Companies should ensure someone is responsible for renewing the company's certification annually, and that they have a reminder set to recertify by the applicable deadline.

- Live up to your Privacy Shield promises. Companies that participate in Privacy Shield are required to substantively comply with the Privacy Shield principles. The FTC has brought enforcement actions against companies that say they comply with the Privacy Shield principles but do not do so in practice. For example, companies may fail to verify annually that their statements about their Privacy Shield practices are accurate, as required under the principles. Companies should make sure they are familiar with the substantive Privacy Shield principles and have documented processes in place to ensure compliance.

COPPA. The Children's Online Privacy Protection Act and Rule (COPPA), which went into effect in 2000 and was last updated in 2013, imposes certain requirements on websites and online services that collect personal information from children under the age of 13. For example, these services must provide notice to parents and obtain verifiable parental consent before collecting information from a child; post a detailed privacy policy; and ensure that the information collected is adequately secured. COPPA was a major priority for the FTC in 2019, and enforcement in this area shows no signs of slowing down in 2020. The FTC brought three COPPA cases in 2019, two of which were the largest COPPA settlements obtained by the agency to date: $5.7 million against Musical.ly, Inc. (now TikTok) and $170 million against Google and YouTube in a joint settlement with the New York Attorney General. We expect the FTC to bring more COPPA cases in 2020 so if you direct your services to children under 13, or knowingly collect information from users under the age of 13, you should think carefully about their compliance obligations. Penalties can be steep: up to $41,000 per violation.

While the FTC continues to enforce COPPA, it has also acknowledged that the Rule may not be keeping up with rapidly changing technology. In July, the FTC announced that it would undertake a review of the COPPA Rule, due to questions that arose regarding COPPA's application to 1) the education tech sector; 2) voice-enabled, connected devices; and 3) general audience platforms that host third-party, child-directed content. In a notice issued July 17, 2019, the FTC sought public comment on a wide range of issues related to COPPA, and held a public workshop to review the Rule on October 7, 2019. The FTC has yet to issue any findings from the public comments or workshop, but we expect to see movement this year.

Key Takeaways:

- Think about your audience. Examine who your service is intended for, and who is actually using it. Companies have different obligations if they are directing their service to children under 13, or if they have actual knowledge that they have collected information under 13. Having a good understanding of this distinction is key to compliance.

- Pay attention to developments in 2020. There is no question that COPPA will be changing, though how much and in what ways remains to be seen. Whether you have determined that your service is subject to COPPA or not, this area bears another look in 2020.

[1] EU-U.S. Privacy Shield: Third review (Oct. 2019), https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6134.

Facebook Settlement. The FTC obtained a record-breaking $5 billion settlement against Facebook for allegedly violating the Commission's 2012 order against the company by deceiving users about their ability to control the privacy of their personal data. The FTC alleged three main violations of the 2012 order: 1) Facebook shared user data with third-party app developers after telling them that they could limit the sharing of their data to certain groups; 2) Facebook did not adequately assess and address risks posed by third-party app developers; and 3) Facebook told users that they could opt-in to the use of facial recognition technology when the setting was on by default. This is the largest penalty ever obtained against a company in FTC history, and is 20 times higher than any privacy or data security penalty ever imposed worldwide. The settlement shows the FTC's willingness to hold companies accountable—and impose harsh penalties—for recurring violations. At the same time, certain commissioners wrote dissenting opinions claiming the penalty and the terms of the order were too lax, stating that the order should have included additional provisions holding individuals accountable. This was not the only case in which some commissioners pressed for individual liability, and we are likely to see more cases naming individuals liable in the future.

Key Takeaways:

- Live up to your promises about the privacy controls available to consumers. If you say you give consumers affirmative choices about the collection, use, or sharing of their data, don't automatically collect, use, or share this data by default.
- Do your due diligence into third parties' security practices before sharing any user data with them.
- The FTC takes violations of its consent orders seriously and is eager to impose hefty fines and strict compliance provisions for such violations in an effort to achieve industry-wide deterrence.

Data Security

The FTC was also busy on the data security front in 2019. It settled a landmark case with Equifax over a 2017 data breach, and generally strengthened the requirements included in standard data security orders.

New Approach to Consent Orders. The FTC shook up its longstanding approach to data security consent orders in 2019. Data security orders now impose significant new requirements relating to the development of information security programs, third party assessments, and corporate governance.

Although the FTC traditionally includes the requirement that companies develop comprehensive data security programs in its orders, it is now including more detail on what safeguards a company is required to implement as part of these programs. This is likely a direct response to the Eleventh Circuit's decision in LabMD, which held that the FTC's data security order was not specific enough to be enforceable.[2]

The FTC also beefed up the third-party assessor requirements it typically includes in data security orders in an effort to increase accountability. Most significantly, the FTC is now giving itself the authority to approve and re-approve third parties chosen to assess comprehensive data security programs every two years. The new orders also require assessors to identify evidence to support their conclusions, such as independent sampling and document review. And assessors are now required to retain documents relating to the assessment and are not permitted to withhold these documents from the FTC on the basis of certain privileges.

The FTC also included new provisions intended to increase corporate governance regarding data security issues. Most notably, the FTC is now requiring senior company officers to provide annual certifications of compliance with comprehensive data security programs to the FTC.

Key Takeaway:

- Companies should anticipate that data security violations may result in settlements that impose these new obligations, which typically remain in effect for 20 years.

Equifax Settlement. In July 2019, the FTC, Consumer Financial Protection Bureau (CFPB), and all 50 U.S. states announced that they settled with Equifax over a 2017 data breach that compromised the names, dates of birth, Social Security numbers, addresses, and other personal information of approximately 147 million U.S. consumers. In its complaint, the FTC alleged that Equifax violated Section 5 of the FTC Act and the Gramm Leach-Bliley Act (GLBA) Safeguards Rule by failing to patch known, critical security vulnerabilities affecting its networks and systems that resulted in the data

[2] LabMD, Inc. v. FTC, 891 F.3d 1286 (11th Cir. 2018). Click here to read our complete WSGR Alert on the LabMD decision.

Continued on page 4...

FTC Trends and Forecasts. . . *(Continued from page 3)*

breach. As part of the settlement, Equifax agreed to adhere to heightened data security requirements and pay $575 to $700 million in monetary relief.

Key Takeaways:

- Heed data security warnings. If you receive a credible alert about potential data security vulnerabilities, particularly vulnerabilities that may affect sensitive data, take action to address those risks.
- Adhere to FTC guidance on data security best practices. For example, make sure you update and patch third party software, monitor activity on your network, and segment your network. The FTC may take the position that you have not implemented "reasonable" data security procedures if you do not follow its guidance on these issues.

Consumer Protection

Finally, the FTC showed increased interest in a number of consumer protection issues. Most notably, the FTC brought a number of cases involving deceptive endorsements, ratings, and reviews. As social media continues to become an increasingly desirable advertising medium for businesses, the FTC will likely continue to focus on these concerns in 2020.

Endorsements and Influencers. The year 2019 saw an increase in the FTC's focus on deceptive endorsements, particularly endorsements on social media. The FTC's Endorsement Guides outline how the FTC Act applies to the use of endorsements in advertising.[3] Among other things, the Endorsement Guides explain that influencers are required to disclose when they receive compensation, such as financial compensation or free or discounted products or services, in exchange for their endorsements. In November 2019, the FTC published materials giving influencers additional guidance on how to comply with this obligation.[4] These materials provide practical tips, such as how to make disclosures in photos and videos, and provide additional guidance, such as whether tags, likes, and pins are "endorsements" subject to the disclosure requirements.

The FTC brought several cases against companies for deceptive endorsements in 2019. For example, the FTC settled with a company and its principals for hiring athletes to post endorsements of its client's new mosquito repellant on social media without disclosing that the athletes were paid for the posts. The FTC also settled with a company and two of its officers for failing to disclose that endorsers who recommending the company's products in ads aired on TV and posted on social media platforms received free products in exchange for their endorsements.

Key Takeaways:

- Influencers should make sure they are familiar with these materials and include appropriate disclosures in their posts if they have a material connection to the brand whose products they're endorsing.
- Companies that use influencers to promote their products or services should have controls in place to ensure their influencers understand and comply with their disclosure obligations, such as contractual provisions and auditing and monitoring procedures.

Ratings and Reviews. The FTC also brought a number of enforcement actions relating to deceptive ratings and reviews. For example, the FTC brought an action against a company for allegedly misrepresenting that customer reviews were independent when in fact it provided customers with free products and other incentives in exchange for posting positive reviews. The FTC also settled with a company that allegedly encouraged its managers and employees to use fake accounts to post positive reviews of its products on a major retail website. Finally, the FTC settled with another company for allegedly paying a third-party website to post fake reviews of its products on Amazon.

Key Takeaways:

- Make sure any ratings and reviews posted by customers who received compensation for their ratings and reviews contain the required disclosures.
- Do not encourage your employees or anyone else to whom you have a material connection to post positive reviews of your products or services.
- Do not pay other companies to post fake reviews of your products or services.

---

[3] 16 C.F.R. Part 255; The FTC's Endorsement Guides: What People Are Asking (FAQs) (Sept. 2017), https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking.

[4] Disclosures 101 for Social Media Influencers (Nov. 2019), https://www.ftc.gov/tips-advice/business-center/guidance/disclosures-101-social-media-influencers.

European Privacy Landscape: What to Expect in 2020

By Cédric Burton, Bastiaan Suurmond, and Josephine Jay

The year 2020 promises to be an interesting one for privacy and data protection in Europe. In this post, we highlight four of the most important developments to watch this year: 1) we expect that European Union (EU) regulators will ramp up GDPR enforcement across the board, and with a particular focus on AdTech, cookies, and children's data; 2) legislators and regulators are looking to take concrete measures on AI; 3) the Standard Contractual Clauses will likely have to undergo major reform to escape the same fate as the now-defunct Safe Harbor Framework; and 4) we expect that the proposed ePrivacy Regulation will move forward or be withdrawn altogether.

Increased Enforcement

As early as 2016, the GDPR was hailed as a game-changer that would reshape the relationship of big tech and other organizations with user data, largely due to the potential for massive penalties of up to 4 percent of a company's global revenue. Despite the steady proliferation of high-profile interrogations of data-rich companies, the expected crackdown has not yet materialized. Investigations are often delayed due to extensive, and often confidential, back-and-forth with the target, or due to court challenges. The Irish regulator, for example, has faced criticism for the long-delayed outcome of its investigations into a number of big tech giants with EU headquarters in Ireland, and the headline grabbing announcements by the UK regulator that it intends to issue record-breaking fines to Marriott International and British Airways have yet to come to fruition. We expect this to change in 2020.

We anticipate that enforcement actions will take a sudden jump this year. Regulators have been busy handling a backlog of complaints from newly empowered data subjects. As the dust begins to settle, and regulators have scaled up in terms of resources, we expect an increase in larger enforcement actions, including both audits and fines. A number of regulators are already laying the groundwork for this increase. In September 2019, the German regulators published guidelines on how they would calculate GDPR fines, and soon thereafter two different German regulators issued multimillion Euro fines.

Raising the Bar on All Things AdTech, Cookies, and Kids' Data

Last year, there was a good deal of interest in and engagement on the interlocking AdTech space and cookies rules, as well as the handling of kids' data. Recent developments indicate that we can expect regulators to crack down hard on companies resisting moves towards compliance. Unfortunately, there is still a great deal of confusion regarding obligations in all three of these areas, making compliance more challenging and enforcement actions more likely.

Guidance was issued by each of the UK, French, German, and Spanish regulators on cookies, and the European Court of Justice (ECJ) delivered its judgement in *Planet49* confirming that active opt-in consent is required to set cookies. While a consensus was reached on some points (including the invalidity of implied consent), divergence still exists, for example on the validity of "cookie walls" and the requirement for consent for first-party analytics cookies. How companies operating cross-border will navigate these inconsistencies remains to be seen.

Along with the cookies developments, in June 2019, the UK regulator issued a call to arms to the AdTech industry giving it six months to engage with and seek solutions to the perceived incompatibility between the GDPR and AdTech operations, with real-time bidding in particular. The UK regulator has made positive statements regarding cooperation with the AdTech community but indicates there are still concerns about current practices. The ICO urges organizations, even ahead of an update on its formal position due early 2020, to take action, embedding privacy by design and preparing management for changes ahead. This requirement for change from individual organizations, combined with a lack of certainty as to the way forward, makes enforcement action likely. The one potential benefit of such actions would be additional clarity regarding compliance obligations.

The use of children's data was a hot topic in 2019, and this shows no sign of letting up. On January 22, 2020, the UK regulator published the final version of its Age Appropriate Design Code. We are also awaiting guidance on kids' data from the Irish regulator. The UK regulator's draft version of the code, published early 2019, met with consternation, with fears that it would lead to an age-gated internet. Although clarifications have been made to alleviate these concerns, a seismic shift in how kids' data is handled is likely.

Continued on page 6...

European Privacy Landscape: What to Expect in 2020 *(Continued from page 5)*

Establishment of Guidelines and Potential Regulation of AI

The year 2020 will see an increase in the scrutiny of artificial intelligence technology (AI), both in the data protection space and otherwise, and an attempt to reach a Europe-wide consensus on ethical AI. A report published in June 2019 by the EU Commission's High-Level Expert Group on AI recommends new regulation to "*ensure adequate protection from adverse impacts*" (concerns include profiling of children, and impact on fundamental rights), and recommends the creation of different "risk classes" to ensure proportionate regulator intervention. The EU Commission has promised that new legislation setting out a coordinated approach on the implications of AI will be presented in early 2020.

Regulators have similarly expressed concerns regarding AI and its impact on profiling and automated decision-making, and its use in other emerging technologies such as facial recognition and deep fakes. The UK regulator, in particular, has focused on this, listing it as one of its three strategic priorities, stressing the importance of privacy by design. It has been working closely with stakeholders to publish a formal consultation paper later this month, with an AI auditing framework and guidance expected in spring 2020.

Despite the effort toward an international consensus on AI, we foresee continued fragmentation across the EU member states, as attempts are made to iron out the tensions between the privacy and ethical risks in AI, and its benefits.

A Shake-Up of the Data Transfer Landscape

In the coming months the ECJ will deliver its verdict on the validity of the EU Standard Contractual Clauses (SCCs) as a means of transferring personal data out of the EU in the Schrems 2.0 case. On December 19, 2019, the Advocate General (AG) issued his non-binding, but indicative, opinion, maintaining that SCCs are valid, but that data controllers, and as a second line of defense, national regulators, should ensure that an analysis is conducted for each data transfer to assess whether the laws where the data importer is located are reconcilable with the SCCs. The AG also expressed concerns regarding the validity of the EU-U.S. Privacy Shield.

We expect the ECJ to closely follow the opinion of the AG in its ruling. Although the AG opinion was in many ways favorable, it left open many issues: a greater burden will be placed on companies and increased regulatory scrutiny of transfers will be encouraged. Although the ECJ is not expected to review the Privacy Shield mechanism, the ECJ's decision may be indicative as to how the General Court of the EU will rule on the future of Privacy Shield in *La Quadrature du Net v Commission*. While the SCCs will remain a valid, albeit more highly scrutinized, method of transfer, Privacy Shield for EU to U.S. transfers could be invalidated, leaving companies no choice but to turn back to the now more burdensome SCCs.

One positive result of the increased pressure on SCCs is that we can expect revised versions of the SCCs to finally make an appearance at some point over the coming year. In the latter half of 2019, the EU Commission was seeking input from organizations on updated SCCs, and the Council of European Union, in its draft position on the Application of the GDPR, called on the EU Commission to update the SCCs to align with recent developments, and for the EDPB to issue new guidance on cross-border transfers.

Continued Lack of Clarity in Relation to the ePrivacy Regulation

We still have no clarity over the future of the long awaited ePrivacy Regulation and expect little movement on this in the coming year. The future of cookies and electronic marketing remain in flux, meaning organizations will need to ensure that they are operating in line with the existing Directive driven regime, which is here to stay for the foreseeable future.

Various versions of the ePrivacy Regulation have been presented to the EU Parliament, most recently by the Finnish presidency, with the latest compromise voted down in November 2019. The incumbent Croatian presidency is expected to propose another version in February. The latest debates highlighted the diverging priorities and opinions of the different member states and EU institutions on a number of issues, including regarding the prevention of child abuse imagery and the validity of "cookies walls." This leaves open questions as to when a new regulation will be agreed upon.

The new EU Commission is left with the choice of either allowing continuous compromises and amendments to be tabled, or withdrawing the draft legislation completely and going back to the drawing board to create an electronic communications bill fit for its new digital aims.

The CCPA Is Here, but Confusion Abounds

By Eddie Holman, Megan Kayo, and Ale Lynberg

With a flurry of email notifications from businesses announcing updates to their privacy policies, the California Consumer Privacy Act of 2018 (CCPA) rang in 2020 with a bang. Despite all the activity related to the CCPA, how businesses have interpreted and implemented its requirements has varied widely. One of the most notable differences in interpretation relates to what constitutes a "sale" under the CCPA. Practices on how to best inform Californians of their new right to opt out of sales of their personal information and how to implement that right also vary across businesses.

The California Attorney General proposed regulations to implement the CCPA, but these have not yet been finalized (and were recently updated). Final regulations may add some clarity to the debate, but they also may raise or leave other questions unresolved. Moreover, with another potential privacy measure that could appear on California voters' ballots this November, any agreement on CCPA compliance may quickly become moot.

All told, 2020 will likely be a big year for privacy legislation and enforcement.

What Is a "Sale"?

To better understand why such a variety of implementations of the CCPA's right to opt out have appeared, we should first briefly recap what it means to sell personal information under the CCPA. The CCPA broadly defines a "sale" to cover any disclosure of personal information to another business or third party for monetary or other valuable consideration. With the definition, the CCPA also provides scenarios in which a business will not be deemed to be selling personal information, including a disclosure of personal information by a business to a service provider where such disclosure is necessary to perform a "business purpose" and the following conditions are met: i) the business has provided notice in its terms and conditions of the use or sharing of that information with a service provider; and ii) the service provider does not further collect, sell, or use the personal information of the California resident except as necessary to perform the business purpose.

In light of the foregoing, the relevant analysis for many businesses is determining the kind of entity to which the business is disclosing personal information. In other words, whether the recipient qualifies as a service provider, which would not be a sale, or as a business or third party, which would be a sale assuming there is some form of consideration involved.

What Kind of Entity Is the Recipient of the Personal Information?

"Service providers" are defined as for-profit legal entities that process information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract that restricts how the receiving entity can retain, use, or disclose the personal information.

Service providers who use personal information received from a business for their own commercial purposes become a "business" with regard to that information, and such disclosures by the business to the service provider would be considered a sale if done in exchange for some form of consideration. As such, an entity may meet the definition of both a service provider and a business as part of the same relationship with another business.

The relevant inquiry, then, for companies sharing and receiving personal information is whether the recipient is using such information for the sharing company's business purposes or for the recipient's own commercial purposes.

Is the Recipient of the Personal Information Using It for a Business Purpose?

The CCPA defines a "business purpose" to mean the use of personal information for the business's or a service provider's operational purposes, or other notified purposes, subject to certain restrictions. The definition provides examples of seven business purposes, including auditing, detecting security incidents, debugging, maintaining accounts, and internal research, among others.

The initial proposed regulations issued by the California Attorney General in October narrowly defined the permissible uses of personal information disclosed by a business to a service provider for a business purpose. Under the recently modified proposed regulations, the Attorney General has expanded the list of exceptions to ways in which a service provider can retain, use, or disclose personal information obtained in the course of providing services to a business and still be considered a service provider. The modified proposed regulations would permit a service provider

Continued on page 8...

The CCPA Is Here, but Confusion Abounds *(Continued from page 7)*

to retain, use, or disclose personal information obtained in the course of providing services (1) to perform the services specified in its contract with the business; (2) to retain another service provider as a subcontractor, where the subcontractor also meets the requirements of a service provider; (3) for internal use to build or improve the quality of its services provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source; (4) to detect data security incidents or protect against fraudulent or illegal activity; or (5) to comply with laws and legal investigations, cooperate with law enforcement, and exercise or defend legal claims. These expanded exceptions add to the debate and shifting landscape regarding what is considered a "sale."

How Are Businesses Implementing the Right to Opt Out of Sales?

Under the CCPA, California residents have the right to opt out of the sale of their personal information, and they must be notified of this right. The proposed regulations require the notice be provided at or before the time of collection of a California resident's personal information.

In addition, the proposed regulations require that a business provide two or more designated methods for submitting requests to opt out, including an interactive form accessible via a clear and conspicuous link titled, "Do Not Sell My Personal Information," or "Do Not Sell My Info," on the business's website or mobile application. The proposed regulations also specify that unlike other consumer requests to exercise their rights under the CCPA, notably the request to access and request to delete their personal information, a request to opt out is not required to be a verifiable consumer request.

Notices of the Right to Opt Out

The CCPA privacy notices that businesses have posted are illustrative of the debate and varied interpretation over what kinds of transactions constitute a sale of personal information.

When informing California residents of their right to opt out of the sale of their personal information, some privacy notices include quotation marks around the word *sale* and caveats around the description of the right. For example, such privacy notices state that the business may disclose certain information about the user of the business' services for purposes that may be considered a "sale" under the CCPA. Similar privacy notices explicitly call out that quotation marks are used around the word *sale* and flag that even if no money changes hands when a business discloses personal information to another business or third party, such as when online identifiers and device identifiers are shared with other businesses to further their own commercial purposes, such a disclosure could be considered a sale under the CCPA.

Other privacy notices provide analysis of particular use cases, notably with regard to interest-based advertising. Such privacy notices acknowledge that an argument could be made that when certain third parties place cookies on a consumer's device, the personal information collected by such cookies constitutes a "sale" under the CCPA. Such privacy notices note that whether information collected from cookies constitutes a sale is an unresolved debate. Accordingly, some privacy notices state that, pending resolution or further guidance form the California Attorney General, such businesses will not treat interest-based advertising as a sale.

Methods for Submitting Requests to Opt Out

The methods that businesses are providing to California residents to exercise their right to opt out of the sale of their personal information also vary.

Many businesses that are taking the position that interest-based advertising is not a sale under the CCPA are directing users to the opt-out tools provided by industry groups, such as the Network Advertising Initiative (NAI), Interactive Advertising Bureau (IAB), and Digital Advertising Alliance (DAA). These tools allow users to signal the members of the respective industry groups to stop sending targeted advertising, but do not impact whether information about the user making the request is disclosed to other entities.

Several businesses have included hyperlinks with the requisite text "Do Not Sell My Personal Information" within their privacy notices, which redirect to web forms that request additional information about the user making the request, purportedly in order to verify that the user is a California resident. Other businesses require that the user making the request log into their account with the business in order to make a request to opt out.

In addition, industry groups are developing tools and frameworks designed to provide participating businesses with a way to sell personal information in compliance with the CCPA. Notably, the IAB has

created the IAB CCPA Compliance Framework,[1] which includes technical specifications and an accompanying service provider agreement designed to provide businesses with assurances that participating publishers provide California residents with the requisite notice and opportunity to opt out of the sale of their personal information and also use personal information in ways that would qualify as business purposes.

Similarly, the DAA has developed a CCPA Opt-Out Tool designed to help publishers, brands, agencies and adtech in the digital advertising supply chain sell personal information in a CCPA-compliant manner.[2] The CCPA Opt-Out Tool includes a text link and green icon for publishers to display on their services to allow California users of such services to opt out of the sale of their personal information.

What Happens Next?

Final Regulations and Enforcement

Attorney General Xavier Becerra published proposed regulations on October 10, 2019; the office received over 200 comments covering more than 1,700 pages during the 45-day written comment period. On February 7 and 10, 2020, the Attorney General proposed modifications to the previously published regulations, which are now open for public comment until February 25, 2020. Once final regulations are issued, the Attorney General's office will transmit a rulemaking action to the Office of Administrative Law (OAL) for review. The OAL then has 30 working days to approve the rulemaking action and file the regulations with the Secretary of State.[3] The CCPA requires the California Attorney General to adopt CCPA regulations by July 1, 2020.

The California Attorney General's office cannot bring enforcement actions prior to July 1, 2020. Nevertheless, Becerra has said that his office will take action regarding activity beginning on January 1, 2020 that violates the CCPA.[4] In a letter to the state legislature in August 2018, Becerra urged for an expanded consumer private right of action to seek remedies for privacy violations because the CCPA substantially increased the need for enforcement resources.[5] Despite resource constraints, the Attorney General specified that early enforcement will focus on companies processing large amounts of sensitive data, as well as the collection of personal information pertaining to minors.[6]

CCPA 2.0 Ballot Initiative

The organization responsible for launching the CCPA ballot measure in 2018, Californians for Consumer Privacy, has already filed a new ballot measure to appear in the November 2020 elections. The proposed ballot measure, the California Privacy Rights Enforcement Act, supplements the CCPA and focuses on data minimization and algorithmic transparency, creates a new class of "sensitive personal information" with enhanced protections, and establishes a new state agency responsible for enforcement and issuing regulations.

In December 2019, supporters of the ballot initiative began collecting signatures. They must collect 623,212 valid and verified signatures by June 25, 2020 to appear on the ballot in the November 2020 election.

Conclusion

It is possible there will be further changes once the final regulations are promulgated by the California Attorney General. Nevertheless, given the wide variations in implementation, companies should evaluate whether they are subject to the CCPA and, if so, put processes in place to comply with the CCPA sooner rather than later.

---

[1] IAB CCPA Compliance Framework for Publishers & Technology Companies (December 5, 2019), https://www.iab.com/guidelines/ccpa-framework/.
[2] Digital Advertising Alliance Do-Not-Sell Tool for Publishers and Third Parties, https://digitaladvertisingalliance.org/digital-advertising-alliance-do-not-sell-tool-publishers-and-third-parties (last visited January 11, 2020).
[3] California Office of Administrative Law, "About the Regular Rulemaking Process," https://oal.ca.gov/rulemaking_participation/.
[4] Koseff, Alexei, California Promises Aggressive Enforcement of New Privacy Law, San Francisco Chronicle, Dec. 16, 2019.
[5] Letter from Xavier Becerra, California Attorney General, to Assemblymember Ed Chau, California State Assembly, and Senator Robert M. Hertzberg, California State Senate (Aug. 22, 2018).
[6] Koseff, Alexei, California Promises Aggressive Enforcement of New Privacy Law, San Francisco Chronicle, Dec. 16, 2019.

Challenges to the FTC's Authority in 2019

By Brett Weinstein, Amanda Irwin, and Kelly Singleton

The Federal Trade Commission (FTC) faced unprecedented challenges to its authority in 2019. As a result of decisions from the Third and Seventh Circuits, the Commission's authority under Section 13(b) of the FTC Act—one of its primary tools in carrying out its consumer protection mission—may be severely limited. Specifically, the agency may face difficulty obtaining restitution or monetary relief in some district courts, and it may even be limited in its ability to obtain injunctive relief altogether in others.

FTC v. Shire ViroPharma, Inc.

In March 2019, a Third Circuit panel held that, "Section 13(b) [of the FTC Act] does not permit the FTC to bring a claim based on long-past conduct without some evidence that the defendant 'is' committing or 'is about to' commit another violation." *FTC v. Shire ViroPharma, Inc.*, 917 F.3d 147, 156 (3d Cir. 2019). The decision eliminates the FTC's ability to successfully challenge in federal courts in the Third Circuit conduct that has ceased and the recurrence of which is not imminent—a significant curtailment of the FTC's enforcement power.

The case arose when Shire ViroPharma, Inc. (Shire) became aware that competing pharmaceutical manufacturers were considering making generic versions of a lucrative drug it manufactured, and, in an effort to delay approval of those generics, flooded the United States Food and Drug Administration (FDA) with meritless filings between March 2006 and April 2012. The FDA eventually rejected Shire's filings and approved the generics, but Shire delayed the availability of the generics for years, thereby reaping hundreds of millions of dollars in profits.

In February 2017, almost five years later, the FTC filed suit against Shire in the United States District Court for the District of Delaware under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b). The FTC sought a permanent injunction and restitution, alleging that Shire's meritless filings were an unfair method of competition prohibited by the Act. Under the relevant portion of Section 13(b):

> Whenever the [FTC] has reason to believe—
>
> (1) that any person, partnership, or corporation is violating, or is about to violate, any provision of law enforced by the [FTC,] and
>
> (2) that the enjoining thereof pending the issuance of a complaint by the [FTC] and until such complaint is dismissed by the [FTC] or set aside by the court on review, or until the order of the [FTC] made thereon has become final, would be in the interest of the public—
>
> the [FTC] . . . may bring suit in a district court of the United States to enjoin any such act or practice. 15 U.S.C. § 53(b).

Shire moved to dismiss, arguing that the FTC's allegations regarding its long-ceased activities failed to satisfy Section 13(b)'s requirement that Shire "is violating" or "is about to violate" the law. The FTC argued that it is enough for the agency to show a past violation and a "reasonable likelihood" of future recurrence. The district court agreed with Shire and dismissed the case.

The Third Circuit upheld the district court's decision, holding that the language of Section 13(b) "is unambiguous; it prohibits existing or impending conduct." The court based its decision on both the plain language of the statute as well as a review of its history. It explained that "[w]hen Congress added Section 13(b), the provision was expected to be used for obtaining injunctions against illegal conduct pending completion of FTC administrative hearings." Additionally, the court reasoned that Section 13(b) was not "meant to duplicate Section 5, which already prohibits past conduct," as discussed below. The FTC unsuccessfully argued that, for decades, courts in a number of circuits have interpreted Section 13(b) to apply when the FTC shows a "reasonable likelihood" of future recurrence. The court was also not persuaded by the FTC's assertion that as soon as potential defendants become aware that the FTC is investigating their activities, they could simply stop engaging in them, rendering them immune from suit in federal court unless the FTC could allege and prove an imminent re-violation.

Pursuant to *Shire*, the FTC cannot successfully challenge in federal courts in the Third Circuit conduct that has ceased and where recurrence is not imminent. However, as the court highlighted, the FTC has multiple instruments in its toolbox to combat unfair methods of competition. For example, Section 5 of the FTC Act provides for administrative proceedings to remedy unfair methods of competition. 15 U.S.C. § 45(b). Under Section 5, if the FTC has "reason to believe" that a person, partnership, or corporation "has been or is using" unfair methods of competition, the FTC can issue an administrative complaint "stating its charges in that respect." The

charges are then adjudicated before an administrative law judge (ALJ). Ultimately, if the FTC believes the respondent is violating the law, it issues a written report and serves a cease and desist order upon the respondent. If a respondent violates a cease and desist order, the FTC may seek a civil penalty of no more than $10,000 per violation. Notably, this is a lengthy and multi-step process that the FTC has avoided by using the Section 13(b) route to go straight to court for injunctive and equitable monetary relief, and the FTC is likely concerned that one of the main consequences of *Shire* will be a restriction in its ability to take advantage of the efficiency provided by Section 13(b).

Although the FTC is likely to continue to use Section 13(b) as one of its primary tools and avoid filing cases in the Third Circuit, the Third Circuit decision in *Shire* is already having broader repercussions. For example, even in some investigations outside the Third Circuit, the FTC has insisted that, in order to enter negotiations with the agency, the target of its investigation must sign a tolling agreement whereby it waives arguments concerning timeliness under Section 13(b).

Although *Shire* represents a significant curtailment of the FTC's authority in at least one circuit, the agency did not file a petition for writ of certiorari with the Supreme Court—perhaps in a bid to avoid an unfavorable Supreme Court ruling—and the decision will therefore stand.

FTC v. Credit Bureau Ctr., LLC

The FTC suffered another blow to its Section 13(b) authority when a Seventh Circuit panel held just five months later that, while Section 13(b) provides for injunctive relief and temporary restraining orders, it does not explicitly or implicitly authorize restitution as a remedy. *FTC v. Credit Bureau Ctr., LLC*, 937 F.3d 764 (7th Cir. 2019). The decision overruled *FTC v. Amy Travel Serv., Inc.*, 875 F.2d 564 (7th Cir. 1989), on which the Commission has relied to obtain monetary relief in consumer protection cases for decades. The Seventh Circuit's decision both upends decades of section 13(b) precedent and creates a split with eight other circuits that have adopted the Seventh Circuit's interpretation of 13(b) in *Amy Travel*.

In 2017, the FTC sued credit monitoring service Credit Bureau Center (CBC) and its owner Michael Brown for allegedly violating the FTC Act and other consumer protection statutes by luring consumers into signing up for subscription credit monitoring services with fake rental property ads and deceptive offers for "free" credit reports. The FTC filed its complaint under section 13(b) of the FTC Act, seeking a permanent injunction and restitution. The district court judge issued a temporary injunction, froze CBC/Brown's assets, and appointed a receiver to manage CBC. Later, CBC/Brown and the Commission filed cross-motions for summary judgment. In its motion, CBC/Brown argued, among other things, that section 13(b) does not authorize an award of restitution. The district court judge ruled in favor of the Commission, holding that CBC/Brown violated the FTC Act and other consumer protection statutes, issuing a permanent injunction, and ordering the payment of over $5 million in restitution.

On appeal, CBC/Brown contested liability, the permanent injunction, and the restitution award. The Seventh Circuit affirmed the district judge's decision on liability and the issuance of the permanent injunction, but vacated the restitution award on the basis that section 13(b) does not authorize restitutionary relief. In doing so, the court overruled its widely-adopted decision in *Amy Travel*, in which it held that section 13(b)'s "statutory grant of authority to the district court to issue permanent injunctions includes the power to order any ancillary equitable relief necessary to effectuate [that] power[.]" In reaching its conclusion, the court primarily looked to the text and structure of the FTC Act and Supreme Court decisions clarifying that courts must consider whether implied equitable remedies are compatible with a statute's express remedial scheme.

First, the court examined the text and structure of section 13(b)'s permanent-injunction provision, which states that "in proper cases the Commission may seek, and after proper proof, the court may issue, a permanent injunction." CBC/Brown argued that section 13(b) does not authorize restitution because it does not mention restitution, while the Commission argued that section 13(b) implicitly authorizes restitution, a reading that the Seventh Circuit endorsed in *Amy Travel*. Ultimately, the court concluded that "nothing in the text or structure of the FTC[] [Act] supports an implied right to restitution in section 13(b), which by its terms authorizes only injunctions."

The court also analyzed the key Supreme Court decisions on implied remedies and the lower-court interpretations of 13(b) that built on these decisions and ultimately led to its decision in *Amy Travel*. The Seventh Circuit found that in its more recent decisions, the Supreme Court adopted a more limited understanding of judicially implied remedies that emphasized that the implied remedies presumption yields where necessary to carry out the intent of Congress or to avoid frustrating the purposes of the statute

Continued on page 12...

Challenges to the FTC's Authority in 2019 *(Continued from page 11)*

involved. Based on these cases, the court concluded that *Amy Travel*'s categorical approach to judicially implied remedies and interpretation of section 13(b) "is no longer viable." Instead, it found that these cases require reading section 13(b) as authorizing only injunctive relief.

On December 19, 2019, the FTC filed a petition for a writ of certiorari asking the Supreme Court to review the Seventh Circuit's decision in *Credit Bureau Center*. This is the only the fifth time in its history that the Commission has represented itself before the Supreme Court. Normally, the U.S. Solicitor General represents the FTC in cases before the Supreme Court, and the FTC may only represent itself if the Solicitor General first declines, as he did here. According to the FTC's petition, the agency took this unusual step, not only because of the resulting circuit split and the "extreme importance of the issue," but also because the Seventh Circuit's decision, "threatens the FTC's ability to carry out its mission by eliminating one of its most important and effective enforcement tools."

The FTC's petition in the Credit Bureau Center case is among three petitions raising Section 13(b) restitution issues before the Supreme Court. In each of the other two petitions, *Publishers Business Services Inc., et. al. v. FTC*, No. 19-507 (filed Oct. 18, 2019) and *AMG Capital Management, LLC v. FTC*, No. 19-508 (filed Oct. 18, 2019), U.S. Solicitor General Noel Francisco argued that the Supreme Court should wait to review the petition until after it has decided *Liu v. SEC*, cert. granted, No. 18-1501 (Nov. 1, 2019), a case already before the Supreme Court, that poses analogous questions under federal securities law. Conversely, the FTC argues in its petition in *Credit Bureau Center* that the case poses a distinct question from the one posed in *Liu*, and that resolving the analogous securities law question would not answer the question presented here.

In its petition, the FTC argues that the Supreme Court should grant its petition because i) the case creates a circuit split; ii) the Court of Appeals' decision is incorrect; and iii) the question presented merits plenary review. First, the FTC highlights that the *Credit Bureau Center* decision is inconsistent with the holdings of all seven other circuits to have considered this issue, the decision overturns prior Seventh Circuit precedent, and questions regarding Section 13(b)'s meaning frequently arise. Second, the FTC argues the Seventh Circuit's decision was based on an incorrect understanding of the term "injunction." The FTC argues that the plain meaning, the *Black's Law Dictionary* definition, and the common usage of the term "injunction" do not support the Seventh Circuit's assertion that an injunction is only forward-looking, nor that it is "obvious" that "[r]restitution isn't an injunction." The FTC also argues the legislative intent of Section 13(b) is consistent with its position based on how courts have interpreted similar laws, pointing to the securities laws authorizing district courts to order the return of ill-gotten gains. Finally, the FTC notes that Congress has amended the FTC Act several times but has chosen not to alter the Section 13(b) language, indicating that Congress approves of the courts' interpretation of Section 13(b) as granting the FTC the ability to seek restitution.

Given the circuit split the case creates and the frequency with which the FTC relies upon its Section 13(b) authority for monetary relief, the Supreme Court may choose to grant certiorari and review *Credit Bureau Center*. However, because *Liu* is already before the Supreme Court and presents an analogous question regarding securities law, the Supreme Court may merely decide *Liu* and leave lower courts to evaluate its applicability, if any, to Section 13(b). If the Supreme Court holds, outright or by implication, that Section 13(b) does not permit federal courts to provide monetary relief as a form of injunctive relief, the FTC would likely have to dramatically alter its enforcement strategy, and companies under investigation by the agency might be more willing to proceed to court instead of trying to settle. In addition, some stakeholders may press Congress to address the narrower read of Section 13(b) through a legislative fix. In May 2019, Commissioner Wilson asked Congress to clarify the FTC's authority under Section 13(b) in her testimony before the U.S. House Energy and Commerce Subcommittee on Consumer Protection and Commerce, noting that "recent decisions have raised questions about our authority that conflict with the clear intent of Congress and long-established case law."

5 Questions Blockchain Companies Should Ask About Privacy

By Amy Caiazza and Libby Weingarten

One of the most significant recent trends in the worlds of technology and financial transactions is the rise of blockchain as the basis for various types of financial and commercial platforms. Blockchain has the potential to transform basic financial transactions and the flow of information—including personal information (**PI**), which may be used, verified, purchased, and sold by companies of all stripes using blockchain. As companies engage in these transactions, they should consider ways their activities may be regulated under U.S. and foreign privacy laws.

At a high level, blockchain is a glorified database. Often described as a "distributed ledger," blockchain is used to record and track information, including, among other things, information about the ownership and transfers of assets. The database tracking this information is copied, verified, and stored on multiple "nodes"—the computers of individual users—so there is no central intermediary holding the data. The advantage of this system is that there is no need to trust the intermediary that would otherwise store and verify the data. In many cases, information about the individual participants who engage in transactions is encrypted; often, participants are completely anonymous to other users.

How might blockchain implicate privacy laws—particularly when PI is encrypted and potentially unreadable by the sponsor of a platform? Many companies are using blockchain to conduct commercial or financial transactions involving their customers. As they do, they need to comply with "know-your-customer" (**KYC**), Office of Foreign Assets Control (**OFAC**), and even anti-money laundering (**AML**) regulations, which often means they need to collect basic PI about individuals—information they store and possibly transmit on a blockchain. In these and other cases, companies' actions may, knowingly or not, trigger privacy laws inside and/or outside the U.S.

Below, we outline five questions that companies using blockchain to store and transmit data about individuals should consider—and discuss with counsel.

1) Am I a financial institution?

In the U.S, a federal privacy law—the Gramm-Leach-Bliley Act (**GLBA**)—applies specifically to "financial institutions." Financial institutions regulated by GLBA are subject to a set of requirements designed to ensure the security and confidentiality of the information they collect. These requirements are broken down into a Privacy Rule and a Security Rule, each with its own set of obligations and procedures that companies must follow to remain compliant with the law.

At a high level, the term "financial institution" encompasses any business, regardless of size, that is "significantly engaged" in providing financial products or services. Certain entities—such as banks, brokers, and investment advisers—are obviously financial institutions. But other, less obvious businesses may be financial institutions as well: in the "traditional" economy, mortgage brokers, nonbank lenders, real estate appraisers, tax preparers, and even courier services can be financial institutions.

Companies using or developing services based on blockchain may become "financial institutions" if they are providing financial products or services by, among other things, offering mechanisms to transfer money, securities, or other assets. Remember that digital assets (**tokens**) are almost always considered securities for purposes of federal law in the U.S. This means that the sponsor of a blockchain-based platform that has issued and sold tokens used for commercial transactions—and therefore is facilitating the use of its financial product for purposes of buying its goods or services—may be a "financial institution." In addition, a company that provides mechanisms for trading or exchanging digital assets for other assets or for dollars or other currency may be a "financial institution." Similarly, companies that distribute tokens for mining, staking, and other purposes may be financial institutions. The possibilities are just about endless.

2) Whom do I share PI with, and for what purpose?

Financial institutions using blockchain may have access to, and the ability to disclose, PI in many scenarios: among others, when they take in users and run KYC, OFAC, and AML checks, and/or take credit card or other financial data to execute transactions, and then use the data they collect to transmit assets from one party to another. The GLBA generally prohibits the disclosure of PI to nonaffiliated third parties without proper notice and opt-out rights, subject to a few enumerated exceptions, so these companies should carefully examine their sharing practices and ensure they are providing proper notices and opt-outs where required.

Even blockchain companies that are not regulated by GLBA—commercial platforms taking advantage of the distributed ledger system, for example—

Continued on page 14...

5 Questions Blockchain Companies Should Ask About Privacy *(Continued from page 13)*

may share data with service providers, advertising partners, or affiliates. More obviously, companies may sell consumer data using blockchain, either as a primary business or as a way to monetize the data they have received for other purposes. And perhaps most significantly, most companies using blockchain share information, including PI, *to the blockchain*, whether in identifying or unidentifiable form.

Companies that are not financial institutions are still regulated under U.S. privacy laws. Under Section 5 of the Federal Trade Commission Act, companies must ensure that they accurately disclose their data practices to consumers, including their data sharing practices. Further, certain transmissions of data, such as the exchange of information for valuable consideration—are subject to California's new privacy law: the California Consumer Privacy Act (CCPA), which requires opt-out rights in certain cases. Generally, it is irrelevant that the PI is encrypted when it is transferred. What matters is that an entity holding PI shares that data with someone else. In such cases, the sharing entity should provide adequate notice of its sharing practices, and examine whether the sharing requires the implementation of an opt-out for consumers.

3) How do I provide notice of my information practices?

As described above, all companies that collect and use personal information must provide notice of their information practices—how they collect, use, and share data. Financial institutions that are regulated by the GLBA have specific obligations under the GLBA's Privacy Rule, which explains how such companies should provide notice, and what that notice must include. Depending on who the company shares personal information with, that notice might change. Among other things, the notice must include:

- Categories of information collected.
- Categories of information disclosed.
- Categories of affiliates and nonaffiliated third parties to whom the company discloses the information.
- A company's policies and practices with respect to protecting the confidentiality and security of personal information.

The notice must also provide information about how consumers can exercise their right to opt out, if such a right is required. For example, financial institutions that share data with non-affiliated third parties must provide an opportunity to opt out, subject to a few enumerated exceptions. GLBA-covered privacy notices must be delivered at the beginning of a new customer relationship, and, unless an exception applies, annually thereafter. Blockchain companies engaged in financial activities should examine their registration flow and other interactions with consumers to determine the best time and place to ensure that users are given clear and conspicuous notice of their information practices.

Companies that are not regulated by GLBA are still required to provide notice of their information practices under various state laws and FTC guidance. These privacy policies should, generally, be clear and conspicuous, accurately detail the company's collection, use, and disclosure practices for personal information, and include additional information for consumers, such as how they can change or access the personal information they provided, and what the company's procedures are for updating the privacy policy.

4) What do GDPR and CCPA mean for me?

Privacy law is evolving at a remarkable rate—with new legislation introduced seemingly daily. In May 2018, the General Data Protection Regulation (**GDPR**) came into force in Europe. The GDPR is an omnibus data privacy regulation that applies to any company established in the European Economic Area (**EEA**) that processes personal information, or any company that processes the personal information of individuals inside the EEA, regardless of the company's location. The GDPR imposes significant restrictions on companies subject to it, covering topics from third party sharing to data breach notification. Among other things, personal information must be processed only pursuant to an enumerated legal basis; data subjects must be given the right to access, correct, and delete their personal information; and companies must implement privacy by design techniques, as well as other accountability measures and documentation of a robust privacy regime.

Most blockchain companies do not, or cannot, limit their activities to the U.S.—and therefore will be subject to GDPR compliance. The best time to think about GDPR compliance is when a company is still in development phase—this way, new features and data uses are evaluated in the context of existing regulations.

Privacy legislation has also made recent headlines in the U.S.: federal privacy bills have been introduced in Congress with bipartisan support, and 2018 saw the introduction of the most comprehensive state privacy legislation to date: the CCPA. The CCPA adopts

many concepts from the GDPR, such as consumer access and deletion rights, detailed privacy notice requirements, and restrictions on the ways service providers may collect and use data. However, as described above, the CCPA imposes additional restrictions on third party sharing—specifically, businesses are required to offer an opt-out if the business "sells" data to third parties. "Sell" is defined very broadly to include any sharing of personal information in exchange for valuable consideration, subject to a few enumerated exceptions.

The CCPA applies to any companies that do business in California and either 1) have gross annual revenues above $25 million; 2) receive or sell personal information of 50,000 or more California consumers, households, or devices; or 3) derive 50 percent or more of annual revenues from selling consumers' personal information. The law is still in flux, with the Attorney General most recently issuing proposed regulations on October 10, 2019, but the main tenets described above are likely to stick.

As with GDPR, blockchain companies should think about CCPA compliance at the earliest stages possible. Considering privacy when building new features or considering possible revenue models is known as "privacy by design," and is required under the GDPR and a best practice under U.S. law.

Update: UK's Age Appropriate Design Code

By Cédric Burton, Lore Leitner, and Josephine Jay

On January 21, 2020, the Information Commissioner's Office (ICO) published its final version of its Age Appropriate Design Code of Practice (the code). The code will be submitted to Parliament in the coming days, and, assuming there is no objection, will become effective approximately two months later.

This article follows our previous update on the ICO's draft Age Appropriate Design Code. The current code was produced following extensive industry and consumer engagement. It adopts the maximum transition period of 12 months to allow companies to make meaningful and thoughtful changes to how they operate.

Clarification on the Code's Scope

Some of the most interesting amendments addressed the controversial scope section, which some contended was paving the way for an age-gated internet.

What services are in scope?

The code applies to any online products or services that *are likely to be accessed* by children (i.e., anyone under the age of 18). This includes applications, websites, search engines, community environments, programs, games, and connected toys or devices. Although the scope remains unchanged, the ICO has now explained what this means in practice. When considering the *likelihood of access* by children, a company should consider:

1. whether the nature and content of the service is particularly appealing for children, and
2. how the service is accessed and the measures implemented to prevent under-age use.

The ICO stresses a common-sense approach:

- Where it is clear cut that a company does not wish children to use its services, it should take steps to verify age (see below on *Age appropriate application*) and prevent access by children so that the code's standards do not apply.
- If conversely a company is specifically targeting children, or the company knows it has a substantive user database under 18, the code's standards will automatically apply.
- In the grey area in between, where a service could be used by children despite them not being the prime target audience, companies should analyze the nature, content, or presentation of the services to assess the extent to which their

Continued on page 16...

Update: UK's Age Appropriate Design Code *(Continued from page 15)*

> services are appealing to children. If a company establishes that children will want to use its service, the standards of the code will apply.

Companies should document decisions regarding the application of the code as this will lead to some level of leniency from the ICO.

Impact of Brexit

The transition period following the UK's exit from the EU is likely to be over by the time the code becomes enforceable. After the transition period, the code will apply to any company targeting or monitoring individuals in the UK, regardless of where they are located. In addition, Elizabeth Denham, the current information commissioner, has stressed that she expects other jurisdictions to use the code as a benchmark.

Key Takeaways

The code sets out 15 headline "standards of age appropriate design" (the standards) that must be implemented. Each of them is accompanied by explanatory guidance, but compliance will be measured against the standards alone. Given the wide range of risk profiles presented by the services covered by the standards (due to both the broad array of services subject to the code and the variety of data processed), the code advocates for a risk-based and proportionate approach. Some of the key takeaways are set out below.

Age appropriate application

Our earlier blog post discussed the requirement to adapt application of the standards depending on the age range a user falls into (i.e., 0 to 5; 6 to 9; 10 to 12; 13 to 15; and 16 to 17). The final code follows the same approach but provides further guidance as to what this means practically.

This standard requires companies to apply all standards to all users (whether they have self-declared as an adult or child), unless they can establish age with a level of certainty appropriate to the level of risk presented by the processing. This would mean, for example, that all users and not just those identified as being children would have their settings set by default to the highest privacy setting. The code offers some guidance on appropriate age verification methods that can be used to verify what age group an individual falls into, ranging from self-declaration for low risk processing to the use of AI.[1]

Strict default privacy settings

Settings for children must be set by default to the highest privacy setting, except if data processing is necessary for the provision of a company's core service. The ICO will carefully review a company's compliance approach if it relies on this exception. The code discusses in some detail situations where this highest privacy setting must be set by default, including a) disclosure (including making visible) of a child's data to a third party, b) the use of geolocation data, and c) profiling.

Even where the child actively opts in to lower privacy settings, the processing must still comply with the General Data Protection Regulation (GDPR) and the child must be protected from harmful effects. For example, companies profiling children to provide recommendations have a responsibility in relation to the recommendations they make. Furthermore, companies should not use "nudge techniques", for example by using certain placements or colors, to "nudge" children to follow the less privacy friendly settings. The code goes further and encourages the use of such "nudge" techniques to guide children to options that protect their privacy, and those that support their health and wellbeing, such as encouraging them to take breaks during gameplay and providing means to save progress.

Caution with "sticky features"

Companies should not use children's data in a way that is detrimental to their wellbeing. This means that companies should exercise caution with "sticky features" (strategies to extend user engagement, such as rewards, notifications, and autoplay features). According to the code, data-driven features that make it difficult for a child to disengage or are addictive, are unlikely to be fair under the GDPR. This includes features that exploit peer pressure.

Next Steps

The Parliament is unlikely to modify the code and we expect that it will remain unchanged. While it will only be enforceable in the next 14 months, companies should consider preparing by assessing whether they are in scope, and by documenting how the standards apply to their users. Then, companies should consider conducting a fuller gap analysis based on the 15 standards, followed by a remediation plan and design changes. Although it may be tempting to wait to see how the market reacts following the transition period, the ICO has stated that enforcement will take into account efforts made during this time.

1 The code interestingly opines that if cookies are used solely for age verification purposes, they can be considered essential under the Privacy and Electronic Communications Regulation, meaning consent is not required.

Schrems 2.0: AG Opines That Data Transfers to U.S. Are Valid Under Standard Contractual Clauses

By Jan Dhont, Laura De Boel, and Laura Brodahl

On December 19, 2019, in the Facebook Ireland and Schrems (Schrems 2.0) case,[1] the Advocate General (AG) to the European Court of Justice (ECJ)—European Union›s highest court—opined that the EU Standard Contractual Clauses (SCCs) are a valid data transfer mechanism to export personal data from the European Economic Area (EEA) to third countries

Businesses encountered major legal uncertainty when the EU-U.S. Safe Harbor mechanism was invalidated following the *Maximillian Schrems vs. Data Protection Commissioner* (Schrems 1.0)[2] case in 2015. The SCCs are a data transfer mechanism relied on by thousands of companies to transfer personal data, and are critical to the flow of personal data globally. While the AG Opinion is not binding on the court, it is a significant development as it may indicate the direction of the final judgment in the case.

Background

In 2013, privacy activist Max Schrems filed a complaint with the Irish Data Protection Commissioner (the DPC) relating to transfers of data from the EU to the U.S. by Facebook Ireland following the Snowden revelations. Schrems alleged a violation of data protection rights as a result of suspected data sharing between U.S. companies and intelligence agencies. In 2015, the ECJ invalidated the EU-U.S. Safe Harbor adequacy decision, which allowed companies to export EU personal data to the U.S. under the EU-U.S. Safe Harbor framework, on the basis that it was not providing an adequate level of protection to EU personal data. Following this, many companies began relying on SCCs for EEA to U.S. transfers, and in 2016 the European Commission (EC) approved a new safe harbor program: the EU-U.S. Privacy Shield Framework.

Thereafter, Max Schrems filed a new complaint with the DPC, this time challenging Facebook Ireland's use of the SCCs as a transfer mechanism. The case made its way to the ECJ, via a reference for a preliminary ruling from the Irish High Court, in 2018. The Irish High Court's referral contained a wide-ranging list of questions focusing on the validity of SCCs in relation to transfers to the U.S. For the full background on Schrems 1.0 and 2.0, please see the WSGR Data Advisor article *And Then There Were None: Or How Schrems 2.0 May Invalidate the Standard Contractual Clauses and the Privacy Shield.*[3]

On July 9, 2019, oral arguments on the referred questions were presented to the ECJ by interested stakeholders, and the AG formulated his response over the intervening five months.

Key Points of the AG's Opinion

SCCs

The AG opined that the SCCs are valid since they are designed to ensure a continuous and adequate level of protection, when personal data is transferred by a company in the EU to another company in a third country. According to the AG, the existence of SCCs in itself compensates for any perceived data protection deficiencies that exist outside the EU.

The AG recognized that the legal context in a third country may make the SCCs' obligations difficult to implement. However, the fact that the SCCs are not binding on third countries' public authorities does not render them invalid. Rather, any foreign law that imposes obligations on the data importers that are at odds with the SCCs emphasizes the burden that controllers and, in the alternative, Supervisory Authorities have when reviewing data transfers. A case-by-case analysis is thus required for each data transfer to assess whether the laws where the data importer is located constitute an obstacle to the implementation of the SCCs. If they do, then the transfers should be prohibited or suspended. As a practical matter, it will be very difficult for data exporters to live up to the requirement to assess whether local law in the data importing country is reconcilable with the SCCs.

[1] Case C-311/18. Press release of the opinion available here: https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165en.pdf. Full text of the opinion available here: http://curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=EN&-mode=req&dir=&occ=first&part=1&cid=47018.

[2] Case C0362/14, available here: http://curia.europa.eu/juris/liste.jsf?num=C-362/14.

[3] Available at: https://www.wsgr.com/en/insights/and-then-there-were-none-or-how-schrems-20-may-invalidate-the-standard-contractual-clauses-and-the-privacy-shield.html.

Continued on page 18...

Schrems 2.0 . . . *(Continued from page 17)*

Privacy Shield

The AG also advised the ECJ not to address the Privacy Shield questions raised by the Irish High Court in this case, as the subject matter of the main proceedings is limited to the validity of the SCCs. However, if the ECJ does decide to examine the validity of the Privacy Shield Framework, the AG opined that this should be done in the abstract and should not affect the findings on the validity of the SCCs.

Nevertheless, the AG provided a detailed analysis,[4] whereby he expressed certain concerns about the conformity of the Privacy Shield with the GDPR. In particular, the AG is doubtful as to whether the U.S. guarantees, in the context of the activities of its intelligence services,[5] offer an adequate level of protection for the privacy of EU individuals.[6] The AG also questioned whether the Privacy Shield offers an effective judicial remedy to EU individuals since the Privacy Shield Ombudsperson does not appear to provide a remedy before an independent body, nor to offer individuals a possibility to exercise their privacy rights or contest infringement of their rights by the U.S. intelligence services.

Implications for Companies

If the ECJ follows the AG's opinion regarding the validity of the SCCs, at first glance there will be little impact for most EU data transfers to third countries. However, companies will need to conduct a case-by-case assessment and ensure that data transfers to third countries conform with the GDPR. In addition, the AG's emphasis on the need for Supervisory Authorities to police data transfers under the SCCs may increase pressure on them to investigate whether transfers made under the clauses actually provides the protection they are supposed to.

If the ECJ follows the AG's recommendation and does not examine the validity of the Privacy Shield, then nothing will change for U.S. companies that rely on the Privacy Shield for their EU data transfers anytime soon. However, if the ECJ decides to address the substance of the Privacy Shield questions it will likely partly or wholly invalidate the framework, given the specific concerns raised by the AG. In this scenario, companies will need to take swift action to rely on SCCs or another adequate transfer mechanism until the EU and the U.S. formulate a Privacy Shield fix or a new data transfer regime.

Next Steps

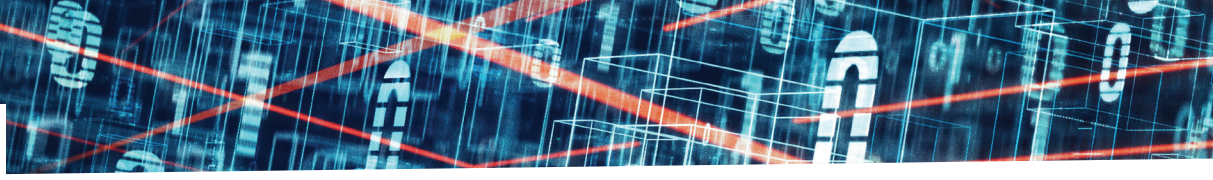
The ECJ will likely issue a final decision on the issues within a few months, and follow the opinions voiced by the AG as it has done in roughly 70 percent of the cases so far.[7] However, as shown in the past when the court invalidated the EU-U.S. Safe Harbor Framework, it can decide to broaden the scope of its review and look at the EU-U.S. Privacy Shield. In addition, in the past the court has sometimes gone against the views of the AG (e.g., in the *Google Spain* case involving the «right to be forgotten» decided in 2014), and there are no guarantees it may not do so here as well.

While the opinion is practical and nuanced with regard to use of the SSCs, it does put the burden on EU companies and Supervisory Authorities. In practice, companies and ultimately regulators will be responsible for assessing whether the SCCs conflict with the law of the data importer, and to potentially suspend or prohibit the transfer of personal data. Companies should now wait for the actual court decision, but should prepare themselves in case the court takes a different view on the SCCs and the Privacy Shield than the AG has done.

Wilson Sonsini will continue to monitor the news and update you once the ECJ decision is published.

---

[4] Paras. 187-342 of the AG Opinion.
[5] Section 702 of the FISA and EO 12333.
[6] Within the meaning of Art 45(1) of the GDPR and Art. 7 and 8 of the Charter of Fundamental Rights of the European Union, and Art. 8 of the ECHR.
[7] An Econometric Analysis of the Influence of the Advocate General on the Court of Justice of the European Union, (2016), Cambridge Journal of Comparative and International Law, Vol. 5, No. 1.



WILSON SONSINI

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com