Privacy and Product Counseling: 2020 in Review

Gerald J. Ferguson, Melinda McLellan and Nichole Sterling
Summary

Advising our clients on compliance with laws and regulations is, hands down, the most important aspect of our role as attorneys. In addition to seeking counsel on their obligations under laws and regulations, however — motivated by industry trends, utilization of and dependence on third-party services and platforms, and, this year, the COVID-19 pandemic — organizations increasingly seek us out for advice on third-party requirements and nonlegal or legal-adjacent issues. While compliance with the California Consumer Privacy Act (CCPA) and addressing issues arising out of the *Schrems II* judgment and the TikTok and WeChat executive orders, among others, dominated 2020, organizations faced an onslaught of other ancillary issues this year on which they sought our advice. Below, we have summarized a list of privacy and product counseling issues on which we have advised our clients this year. This is, of course, not an exhaustive list, but rather highlights some of the bigger privacy and product counseling issues our clients have faced, and on which we have advised them, in 2020.

Advising on these issues is a key part of our privacy and product counseling practice, which spans a number of our Digital Assets and Data Management (DADM) Practice Group teams, including our Privacy Governance and Technology Transactions, Advertising, Marketing and Digital Media, and Digital Transformation and Data Economy teams.
COVID-specific Legal Issues

As discussed below, the effects of the COVID-19 pandemic have been wide-ranging, spurring businesses into organizational changes, shifting state legislatures’ attention away from privacy-related legislation and almost preventing the CPRA from making it onto the 2020 ballot. Businesses also dealt with the direct effects of COVID-19 and compliance requirements that flowed from it. Throughout 2020, our clients turned to us, and they continue to turn to us, as their trusted advisers to address these issues, including state and local shutdowns, return-to-work and other employment-related compliance, bankruptcy and reorganization counseling, and many other issues, as highlighted in our Coronavirus (COVID-19) Resource Center. We also provided key advice to clients, including regarding implementing contact tracing mobile applications, advertising personal protective equipment and other COVID-related products, and pivoting and transforming digital assets into alternative revenue streams.

Privacy and Data Security Laws and Regulations

CCPA. The California Consumer Privacy Act (CCPA) dominated much of the conversation in the privacy and product counseling space this year. Jan. 1, the effective date of the CCPA, came and went after organizations spent much of 2019 addressing the CCPA’s statutory requirements and the first round of regulations from the Office of the Attorney General (OAG). For the first half of 2020, the OAG kept everyone on their toes, issuing multiple rounds of modifications to the regulations before submitting final regs to the Office of Administrative Law on June 1. The regs were then not finally adopted until August 14.

And just when we thought the OAG was done with the regulatory process, his office introduced further regs in October and December (in the latest draft, the OAG has proposed a new “Do Not Sell” logo along with regulations that make it unclear whether or not the logo is required). While there have been no public CCPA enforcement actions by the AG in 2020, we are aware of multiple ongoing investigations in which the OAG is inquiring about website owners’ use of interest-based advertising cookies and their lack of a Do Not Sell button. It is unclear whether the OAG will make any of these enforcement actions public. What is clear is that businesses will have to address CCPA cookies compliance in a robust manner in 2021, if they have not already. BakerHostetler attorneys, many of whom have expertise in AdTech and the related privacy issues, have worked with scores of clients on compliance with cookies and interest-based advertising issues, and were involved in the development of advertising industry opt-out tools, discussed in further detail below.

For a comprehensive listing of our CCPA blog posts, please visit here.

CPRA. On Election Day 2020, California voters approved a ballot measure, Proposition 24, known as the California Privacy Rights Act of 2020 (CPRA), brought by the same group of individuals that were ultimately responsible for the original introduction and passage of the CCPA. Referred to by some as CCPA 2.0, the CPRA will amend certain provisions of the paradigm-shifting 2018 California Consumer Privacy Act (CCPA), as companies were just figuring out how to comply with the CCPA. Among the highlights are extension of the HR and B2B exemptions through Jan. 1, 2023; a new, stand-alone privacy agency tasked with issuing regulations and administrative enforcement of the law; significant amendments implicating AdTech and cookies compliance (including a new definition of “sharing” in the context of “cross-context behavioral advertising”); limitations on and disclosure requirements relating to businesses’ retention of personal information; and new limitations on purposes of processing to those that are “necessary and proportionate.” Our blog post discussing the significant provisions of the CPRA can be found here. Like everything in 2020, the CPRA faced COVID-related woes with respect to collection of the requisite number of signatures to make it on the ballot, as we discuss in a blog post.
California’s Shine the Light Law. California’s Shine the Light law (Cal. Civ. Code Section 1798.83) continues to exist alongside the CCPA. Companies and lawyers alike had to knock the dust off this early 2000s, dot-comera law in order to harmonize positions as to whether a company “sells” personal information under CCPA and shares personal information for third parties’ “direct marketing purposes” under Shine the Light (though this is a very nuanced issue that requires analysis on a case-by-case basis).

Nevada’s SB-220. Taking effect in fall 2019, this amendment to Nevada’s existing data privacy law includes a “Do Not Sell” right that is much more limited in scope than the one found in the CCPA. Unlike the CCPA, a “sale” under SB-220 only covers personal information collected online and requires a direct payment of monetary consideration, and requires that the purchaser onward sell or license the data. Moreover, “covered information” and “operator” are narrower than the CCPA’s concepts of “personal information” and “business,” respectively. For our Baker Data Counsel articles on SB-220, visit here.

COPPA. 2020 saw its fair share of movement in children’s privacy issues, including (1) an update to the FTC’s Children’s Online Privacy Protection Act (COPPA) FAQs (integrating new guidance on age gates, connected toys, the Internet of Things, audio recordings and new methods of verifiable parental consent approved by the FTC), (2) the intersection between the COPPA and the CCPA, (3) bills that sought to increase the protection of children’s privacy, such as the Parent’s Accountability and Child Protection Act introduced in California (which sought to place additional obligations on social media platforms collecting personal information from children under the age of 16, but was vetoed by the governor) and the usual annual federal bills seeking to revise COPPA, (4) enforcement action settlements related to misrepresentations about membership to a COPPA safe harbor program and collection of persistent identifiers, and (5) FTC guidance on COPPA compliance for EdTech companies and schools in the midst of a pandemic. Children’s privacy and related children’s issues, such as data related to loot boxes and increase of collection of children’s information as remote learning and play-at-home practices continue through the pandemic, will likely keep regulators’ and legislators’ attention. BakerHostetler attorneys regularly advise companies on how to navigate such a sensitive issue while also keeping an eye on future developments to the enforcement and legislative landscape. For a list of our blog posts on children’s privacy, please visit here and here.

Other State Privacy Legislation. BakerHostetler attorneys routinely advise on other state privacy and data security laws, including other California laws such as CalOPPA, and Delaware and Massachusetts privacy laws.

In 2020, numerous states introduced privacy legislation, and passage of these sweeping privacy laws in at least a couple of those states, including New York and Washington, seemed likely. Some of the bills were CCPA or GDPR inspired; some were as comprehensive as those regulations while others were more watered down. Following the onset of COVID-19, many state legislatures shifted their focus to the pandemic response and failed to advance or pass the introduced privacy legislation. It will remain to be seen if New York, Washington, New Jersey and other states pick up where they left off in early 2021 and attempt to pass comprehensive privacy legislation as their priorities shift away from COVID-19.

Cybersecurity. The FTC and at least half the states require businesses that own, license or maintain personal information to implement and maintain “reasonable security procedures and practices.” Increasingly, clients seek out BakerHostetler attorneys to counsel them through privacy and security by designing frameworks as they build out new products and applications, and to advise on data security issues arising out of vendor and other third-party relationships and in relation to development of internal data security safeguards.
International Laws and Regulations and Geopolitical Issues

Schrems II. In a closely watched July 2020 opinion on the Schrems II case, the Court of Justice of the European Union (CJEU) invalidated the EU-U.S. Privacy Shield Framework, an adequacy decision approved by the European Commission in 2016 that had provided many companies with a mechanism for the lawful transfer of EU personal data to the United States.

The Schrems II decision also called into question the validity of standard contractual clauses, another popular data transfer mechanism, citing U.S. government surveillance activities generally and the lack of effective remedies offered to EU data subjects whose personal data was transferred to the United States. The CJEU’s opinion already has had, and will continue to have, a wide-ranging effect on personal data transfers from the EU to the United States, requiring enhanced technical and organizational measures, reassessment of data flows, and the renegotiation of data transfer provisions. For several months, companies were left in limbo by a lack of meaningful guidance from EU data protection authorities, including the European Data Protection Board (EDPB), on how to comply with the GDPR’s data transfer requirements in light of the Schrems II decision.

Recent draft guidance from the EDPB and draft updated standard contractual clauses from the European Commission have offered some clarification, but it seems likely this will remain an area of intense focus throughout 2021, particularly for U.S. companies engaged in cross-border data transfers with the EU.

GDPR. While the Schrems II decision has dominated much of the discussion about EU data protection in the second half of 2020, several other developments deserve mention.

Brexit. While the United Kingdom officially left the EU on January 31, 2020, a transition period currently applies until December 31, 2020, during which the United Kingdom remains subject to EU law for various purposes, including application of the GDPR. Reports on the Brexit deal indicate that the European Commission is still working on a potential adequacy decision for the United Kingdom, but any adequacy decision will not be in place when the transition period expires. A limited-term transitional adequacy period with regard to data transfers will be implemented under the draft Brexit deal. During this transitional adequacy period of up to 6 months, data transfers to the United Kingdom will not be treated as transfers to a third country and can continue freely.

In 2021, businesses operating in the United Kingdom will need to address the United Kingdom separately from the EU for compliance purposes, understanding that, although similar to the GDPR, the amended UK Data Protection Act will begin to apply this year and has some distinct requirements. Organizations that had designated the UK’s DPA (the ICO) as their lead supervisory authority under the GDPR must determine which, if any, EU Member State may now serve in this capacity. Additionally, companies whose Binding Corporate Rules were approved by the UK’s ICO will need approval from a new (EU Member State) supervisory authority to remain valid, according to an EDPB note published in July. While we await a decision on whether the European Commission will recognize the United Kingdom as “adequate” for purposes of personal data transfers, organizations should consider appropriate personal data transfer safeguards to address data flows between the EU and the United Kingdom, as well as onward transfers from the United Kingdom to other countries, such as the United States. The implementation of alternative data transfer mechanisms has also been encouraged by the UK’s ICO, which will be updating its guidance for businesses to reflect changes in the Brexit deal.

COVID-19. Balancing the protection of personal data against the need to implement effective coronavirus mitigation strategies has been a key concern in debates about pandemic control efforts in Europe, with the EDPB releasing a statement confirming that “emergency is a legal condition which may legitimize restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period.” A follow-up statement from the EDPB emphasized the validity and applicability of the GDPR even in emergency situations.
In connection with the pandemic response, various DPAs and the EDPB issued guidance touching on the protection of personal data in the context of telecommuting, health-related and contact tracing apps, temperature monitoring, and the use of location data. The EU’s eHealth Network ultimately released a Toolbox for use in the development of contact tracing apps, which came with European Commission guidance for protecting personal data when developing such apps.

**Cookies.** Google’s compliance with and adoption of the TCF 2.0 certainly spurred organizations’ compliance efforts and requirements with respect to cookies in 2020. Additionally, regulators across the European continent made waves on the issue. The French Data Protection Authority (the CNIL) finalized its guidelines on cookies and tracking technologies, adding recommendations on obtaining consent, and announced that the use of cookies would be part of its 2020 inspection plans continuing into 2021. A part of the CNIL’s guidelines banning cookie walls was struck down by a French court in July. Recently, the CNIL has issued several large fines related to the failure to obtain consent for the use of nonessential cookies. The Belgian DPA also released guidance on cookies and tracking technologies this year, while the EDPB updated its guidelines on valid consent under the GDPR. The German Federal Court of Justice issued an opinion addressing cookie consent issues in the Planet49 case, which it previously referred to the CJEU, and confirmed that consent is not valid if the consent box is prefilled.

**Regulatory Enforcement.** We have continued to see large fines issued by various EU DPAs this year, including the following:

- **February 2020** – the Italian DPA fined a telecommunications company just over €27.8 million for unlawful marketing practices, such as not maintaining its opt-out list appropriately, failing to manage its marketing call centers, and requiring consent to marketing communications for access to certain deals and sweepstakes. The Italian DPA issued fines on other telecommunications companies in July 2020 for €16.7 million and in November 2020 for €12.2 million related to unsolicited marketing communications.

- **June 2020** – France’s highest administrative court upheld the CNIL’s fine of €50 million on a technology company for failure to obtain valid consent and to provide a transparent, easily accessible notice.

- **July 2020** – the Belgian DPA fined a technology company €600,000 for non-compliance with an individual’s requests under the right to be forgotten. The Swedish DPA fined the same company €5 million for a similar violation.

- **October 2020** – The German Hamburg DPA fined a retailer €35.3 million for illegal employee monitoring practices regarding detailed notes taken and kept in an online system by managers about employees’ personal lives.

- **October 2020** – The UK DPA issued over €40 million in combined fines on several companies related to reported data breaches.

- **December 2020** – The French DPA issued €135 million in combined fines on three companies for failing to give adequate notice about the use of cookies, failing to obtain appropriate consent before setting advertising cookies and failing to provide appropriate opt-out mechanisms for cookies.

**Surveillance.** In October, the CJEU decided several joined cases confirming that EU law precludes national legislation that requires “a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data for the purpose of combating crime in general or of safeguarding national security.” Such surveillance is allowed only when there is a serious, genuine, and present or foreseeable national security threat. Even in such instances the retention of data must be limited both in scope and duration to that which is strictly necessary.
As we head into 2021, companies should note that the European Commission recently issued proposals for a Regulation on European Data Governance aimed at increasing data sharing within the EU, a Digital Services Act that would in part overhaul the eCommerce Directive and a Digital Markets Act to prevent unfair competition in digital markets. These proposed pieces of legislation are worth watching in the new year.

**Chinese-based Business Executive Orders.** In August 2020, the U.S. government issued prohibitions against certain activities related to TikTok and WeChat and their Chinese owners, based on national security concerns that the Chinese Communist Party could access the vast amounts of U.S. citizen data these apps collect. While these prohibitions are being hotly contested in court and are not likely to go into effect until early 2021 at the earliest, if ever, they could ban a wide range of activities and will target a wide range of data (e.g., geolocation data, communications, financial information and health information). Companies that collect, maintain or use U.S. citizen data should therefore carefully review current and potential business partnerships that directly or indirectly involve Chinese persons. BakerHostetler attorneys have been advising such companies on these risks and others, including those related to foreign investment from China – in 2020, an inter-agency national security review of foreign investments in the United States required TikTok’s Chinese owner to divest from the app, and the U.S. government implemented a new law significantly expanding the executive branch’s authority to review and potentially block foreign investments that could result in foreign access to the sensitive personal data of U.S. citizens. Companies doing business with Chinese entities or individuals should continue to pay close attention to this issue.

**Non-Privacy and Data Security Laws and Regulations**

**Digital Millennium Copyright Act (DMCA).** As more and more clients develop interactive web services, the DMCA is more relevant now than ever before. Businesses that host and publish user-generated content on their digital properties must designate a DMCA agent to receive notifications of claimed infringement and put in place a robust DMCA policy. Having a complete DMCA policy and responding to takedown requests “expeditiously” is crucial to protect a business from potentially massive copyright infringement judgments due to user-generated content. BakerHostetler attorneys provide product counseling on the DMCA to companies ranging from startups to big tech.

**Communications Decency Act (CDA).** Alongside the DMCA stands the other bastion of the Internet: the CDA. Although currently in the spotlight politically due to the current administration’s focus on Section 230 and the immunity for large social media platforms, the CDA continues to provide strong protection from liability for what a website’s users say and do on the website, and BakerHostetler attorneys have been there to defend our clients using the law whenever possible. While we are monitoring the advancements with respect to the CDA, it seems unlikely that the current conversation about limiting online platforms’ immunity will continue beyond the current administration.

**Telephone Consumer Privacy Act (TCPA).** Due to the private right of action, the TCPA can be a minefield for businesses that carry out text messaging campaigns or otherwise make automated calls or text messages. In response to COVID-19, more businesses have turned to text to facilitate curbside pick-up and deliveries, and to reach out to customers to promote sales. Pharmacies and medical facilities are planning to use text to assist with vaccine rollout. We frequently counsel clients through various aspects of the TCPA, including procedures and disclosures for obtaining consent, advising on situations where exceptions to the consent requirements apply, drafting mobile phone opt-in and opt-out disclosures, engaging vendors, and revising online terms to apply class action waivers and limitations of liability to SMS programs. Like many years, 2020 was rife with TCPA litigation. On Dec. 8, the Supreme Court heard oral arguments in a case over the definition of “auto-dialer,” on which the federal circuits are split. The Court’s holding, forthcoming in 2021, will certainly have long-standing effects with respect to TCPA jurisprudence generally as well as companies’ compliance with the law.
Industry and Platform Tools, Initiatives and Self-Regulation

Key to our product counseling practice is understanding the technical and legal intricacies of developments in and updates to industry and platform tools, initiatives and requirements. Moreover, many of our clients are subject to advertising industry self-regulation.

Digital Advertising Industry CCPA Opt-Out Tools. To address the CCPA’s novel “Do Not Sell” right, two industry organizations – the Interactive Advertising Bureau and the Digital Advertising Alliance – developed mechanisms by which consumers may opt out of the sale of their personal information in the context of digital advertising. The viability of these programs is currently being tested in multiple OAG inquiries. In addition to counseling clients on CCPA compliance, multiple BakerHostetler attorneys were among the stakeholders engaged by the IAB in the development of its CCPA framework and a digital advertising industry CCPA compliance survey. BakerHostetler’s involvement with the IAB and the efforts in regard to its Framework and industry is a product our firm’s position as a leader in the digital media, advertising and privacy space.

iOS 14 Updates. This summer, Apple announced two new consumer-oriented privacy features. The first, which has been implemented, requires app publishers to disclose information regarding their apps’ data collection and use practices in what some are referring to as a privacy “nutrition label.” Another significant privacy feature, not yet implemented, will require businesses to assess whether they are “tracking” users of their apps and, if so, to obtain opt-in consent from users to continue the practice. You can read our blog post introducing these requirements here.

Google’s Integration with IAB Europe’s GDPR Consent Framework (TCF 2.0). After over two years of operating independently from the IAB Europe’s Transparency and Consent Framework (TCF), Google integrated with the IAB’s TCF 2.0 in August 2020. BakerHostetler attorneys counseled numerous clients that depend on Google’s advertising services through the changes associated with Google’s adoption of the TCF 2.0.

Industry Self-Regulation Updates. The Network Advertising Initiative, a leading advertising industry organization whose members include advertising technology companies, updated its Code of Conduct in January 2020. BakerHostetler attorneys not only counseled NAI members through the updates to the 2020 Code, but provided counsel to customers and clients of NAI members, to which the NAI code requirements apply contractually through their contract with their NAI member-advertising technology vendors. The NAI is already considering further updates to the code, illustrating how quickly things are changing in digital media and advertising.

Data Inventory and Consumer Rights Vendors and Platforms. Many of our clients depend on third-party data inventory and consumer rights management platforms. As a result, it is impossible to advise organizations on compliance with privacy laws like the CCPA and GDPR without being versed in the vendor products our clients use for the same. We have a working knowledge of or expertise in many of these platforms, so our attorneys are able to help our clients operationalize the requirements of the CCPA and other privacy laws. A number of BakerHostetler attorneys went through extensive training on OneTrust’s data mapping and consumer rights management tools.
Cookie Inventory and Management Platforms. Addressing cookies and other tracking technologies, and taking a proper inventory of them on online and mobile properties, is a key part of complying with data privacy regimes, including the CCPA and GDPR. BakerHostetler attorneys and individuals from our industry-leading IncuBaker team conduct assessments of our clients’ cookie inventories using both widely adopted tools and proprietary methods. The assessment includes identification of cookies and how to address them from a compliance perspective on an individual basis. In addition, we are adept at counseling clients through the adoption of cookie consent management platforms, such as OneTrust.

Teleworking Platforms. As companies migrated to or upped their presence on video conferencing platforms, BakerHostetler attorneys fielded questions from and advised clients on various issues relating to companies’ increased telepresence and use of such platforms. Such issues include but are not limited to whether companies can record meetings and what kind of notice is required if they do; whether a company should provide notice of such recordings in their calendar invitations and what the language of the notice should be; how the recordings fit into the company’s existing data retention policy; and many more.

e-Commerce Issues. Motivated by the mandatory closing of brick-and-mortar retail required by state and local quarantine efforts, and consumers’ ongoing reluctance to visit shops and restaurants in person due the COVID-19 pandemic, businesses without an e-commerce presence attempted to move quickly to establish one, while businesses with an existing e-commerce presence hastily moved to expand it. Moreover, restaurants without delivery, curbside pickup, and online and mobile ordering attempted to quickly pivot and expand to provide those capabilities.

BakerHostetler attorneys assisted scores of clients in the expansion of their e-commerce capabilities, including by negotiating contracts with e-commerce and food ordering/delivery platforms, counseling organizations through the legal issues associated with development of e-comm mobile and web applications, drafting terms of use and privacy policies, and providing general counseling relating to the COVID-19-related risks associated with the expanded e-comm activities. BakerHostetler’s cross-disciplinary groups of attorneys from our Privacy Governance and Technology Transactions team and our Advertising, Marketing and Digital Media team have extensive experience in this space and are well poised to advise on all aspects of organizations’ e-commerce activities.

Look for future blog posts on these types of issues. For more information, please feel free to reach out to the authors or others in BakerHostetler’s DADM Practice Group. For additional articles covering the CCPA, the CPRA or the recent Schrems II decision, visit BakerHostetler’s Data Counsel blog and our Consumer Privacy Resource Center.

Barbara Linney, Alan Friel, Carolina Alonso, Orga Cadet, Patrick Waldrop, and Veronica Reynolds also contributed to the drafting of this Review.
Recognized as one of the top firms for client service, BakerHostetler is a leading law firm that helps clients around the world address their most complex and critical business and regulatory issues. With six core practice groups – Business, Digital Assets and Data Management, Intellectual Property, Labor and Employment, Litigation, and Tax – the firm has nearly 1,000 lawyers located coast to coast. For more information, visit bakerlaw.com.

Baker & Hostetler LLP publications inform our clients and friends of the firm about recent legal developments. This publication is for informational purposes only and does not constitute an opinion of Baker & Hostetler LLP. Do not rely on this publication without seeking legal counsel.

© 2021 BakerHostetler