The Toy Association White Paper on Privacy & Data Security: New Possibilities and Perils

Third Edition

March 9, 2017

Sheila A. Millar
Tracy P. Marshall
Nathan A. Cardon
KELLER AND HECKMAN LLP
1001 G Street, N.W., Suite 500 West | Washington, D.C. 20001

Table of Contents

Foreword

This Third Edition of The Toy Association Privacy and Data Security White Paper builds on the informational framework from earlier editions and identifies issues and challenges for the toy industry in 2017 and beyond as we enter a newly uncertain political era. Prior editions centered on specific foundational policies and their effects. In this edition, we organize the discussion around the key emerging trends of principal interest to the toy industry: the growth in the popularity of mobile internet and connected devices, associated vulnerabilities, and the upcoming entry into force of the European General Data Protection Regulation (GDPR) with its still-unknown obligations to protect children's privacy.[1] We retain background materials on topics such as the Children's Online Privacy Protection Act (COPPA)[2] Rule[3] in the appendices, but highlight important political and enforcement developments since the last edition.

[1] Regulation 2016/679 (Apr. 27, 2016).

[2] Pub. L. 105–277, 112 Stat. 2,681 (Oct. 21, 1998), *codified at* 15 U.S.C. §§ 6501–06.

[3] 16 C.F.R. Part 312.

I. Introduction: Major Technological Trends and Developments Affecting the Privacy and Security Debate

The exponential growth in the number of connected products has captured attention from privacy and security advocates and consumer and data protection agencies around the world. The media seems awash in reports of privacy and security vulnerabilities of connected toys and children's products (often inaccurate or exaggerated), including assertions that "Big Brother" is always on and always tracking kids. Against this backdrop, multiple initiatives to develop privacy and security standards for connected products of all kinds have been ongoing. The political transformation brought about by the November elections will have ramifications that are unknown, and we also highlight some possible implications as well.

The app explosion. Since their introduction in the mid-2000s, mobile apps have come to rival, and, in many cases, surpass websites and traditional computer games in importance to users, brands, and publishers. Consumers reportedly use 26 to 27 apps and spend more than a day and a half each month (37 hours and 28 minutes) on the millions of apps uploaded to various platforms and devices.[4] Estimates of screen time use by children suggest that they spend 6 or more hours each day watching television or using computers, tablets, game consoles, or phones.[5] Apps are therefore crucial to companies offering connected products and services to today's consumers, including children.

Makers of devices and operating systems continue to create new ways for consumers to use their connected devices and interact with each other, while consumer applications for virtual and augmented reality seem to be catching on. Major companies are investing heavily in AR and VR technologies. As these technologies proliferate and are incorporated into toys and games, the prospect that they may further blur lines between commercial and entertainment content will almost certainly draw more criticism.

The Internet of Things. The "Internet of Things," or IoT, is exploding, made possible by broader availability of wifi, reduced cost and ease of incorporating wifi chips into everyday devices, and the release of platforms supporting control of individual devices and families of devices. IoT is also sometimes referred to as the

---

[4] *See So Many Apps, So Much More Time for Entertainment*, Nielsen Newswire (June 11, 2015), http://www.nielsen.com/us/en/insights/news/2015/so-many-apps-so-much-more-time-for-entertainment.html (last accessed Oct. 7, 2016).

[5] *See* Jane Wakefield, *Children spend six or more hours a day on screens*, BBC News (Mar. 27, 2015), http://www.bbc.com/news/technology-32067158 (last accessed Oct. 7, 2016).

"internet of everything (IoE)" or cyber-physical systems (CPS). As the National Institute of Standards and Technology (NIST) has noted:

> [CPS] are smart systems that include engineered interacting networks of physical and computational components. These highly interconnected and integrated systems provide new functionalities to improve quality of life and enable technological advances in critical areas, such as personalized health care, emergency response, traffic flow management, smart manufacturing, defense and homeland security, and energy supply and use.[6]

While there is no agreement on a common definition of either the term IoT or CPS, the great promise of connected devices is that they are "smart." An oven can turn off remotely when food is done cooking. Energy-consuming appliances can time their functioning to minimize load on the grid. Smart cars may drive themselves or adjust to avoid an accident. And, like the old "Jetsons" cartoons, we'll be able to tell things what to do through voice-activated technology without lifting a finger.

The ability to gather many disparate bits of information about individuals through apps and devices complicates notions of privacy and traditional distinctions, at least in the U.S., between personal and non-personal data. Additionally, in the U.S., an individual's public activities have been considered fair game for many data collection purposes. Recent court cases are, however, starting to undermine that traditional notion,[7] and that trend may extend to communications that use third parties.[8] In Europe, businesses will face new complexities about how to balance the right to know and speak with the novel "right to be forgotten." At the same time, smart products that collect audio and video information are increasingly likely to be sought by police prosecutors and government authorities for various investigatory and national security purposes. This happened most recently when prosecutors investigating a murder sought data potentially captured through an Amazon Echo device.

---

[6] Cyber Physical Systems Public Working Group, *Framework for Cyber-Physical Systems, Release 1.0* 1 (May 2016), *available at* goo.gl/F6tyFK.

[7] *See, for example, United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945 (2012) (finding that even though traditionally, tracking a vehicle on public roads was not a violation of the Fourth Amendment, warrantless use of a tracking device to monitor movements on public streets was a violation).

[8] *See id.* (Sotomayor, J., concurring) (questioning the "third party doctrine," which holds that individuals have no reasonable expectation of privacy in information voluntarily disclosed to third parties).

Disappearing distinction between "personal" and "non-personal" data. For over a decade, privacy and consumer groups have argued that "interest-based advertising" (IBA) poses privacy risks, and several years ago succeeded in changing the terminology to the less consumer-friendly term "online behavioral advertising" (OBA). Companies' enhanced ability to obtain data and connect databases of information has created uneasiness about tracking users online and has caused distinctions between "personal" or "personally identifiable information" (PII) and "non-personally identifiable information" (non-PII) to erode. The first regulatory signals that the distinction was breaking down were the changes to the definition of "personal information" in the 2013 update to the COPPA Rule. The FTC included IP addresses and device identifiers as "personal information" except when used to support internal operations. More recently, Federal Communications Commission (FCC) rules governing broadband blurred the traditional line between the two,[9] although these rules are almost certain to be rescinded in the early months of the Trump Administration. Regardless of what happens at the FCC, dissolving distinctions between personal (protectable) and non-personal data are creating broader obligations to treat almost all data with special measures, particularly because the EU does treat IP addresses, device identifiers, and similar information as "personal" under the current EU Data Directive and the soon-to-be-implemented General Data Privacy Regulation.

Data breaches and cybersecurity. The internet made it easy to instantaneously communicate across the globe, as well as to collect, transmit, combine, and use vast amounts of information. But with more people connecting to the internet, using ever-increasing numbers of devices, the threats to privacy and security have multiplied. Problems that have existed in the real world, including authentication of communications sent at a distance (think military orders or bank transfers), are replicated on the internet and must be resolved within fractions of a second for the communications to be useful. What is more, simple flaws hidden in code layers beneath a user-friendly graphic interface can open up otherwise secure transactions and communications, including some of the basic building blocks of the internet, such as secure sockets layer encryption.[10]

---

[9] *See* FCC, *Final Rule: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, 81 Fed. Reg. 87,274 (Dec. 2, 2016), *to be codified at* 47 C.F.R §§ 64.2001–12.

[10] *See, for example*, United States Computer Emergency Response Team (US-CERT), *OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160)*, Alert (TA14-098A) (Apr. 8, 2014, last updated Oct. 5, 2016), https://www.us-cert.gov/ncas/alerts/TA14-098A; *see also* XKCD, *Heartbleed Explanation*, https://xkcd.com/1354/.

With hackers, criminals, and state actors looking to access information, data breaches have reached new highs. Yahoo announced in mid–December 2016 that perhaps a billion consumer records were compromised. This is on top of an earlier hack affecting 500 million customers.[11] Even before the Yahoo announcement, breaches affecting millions of consumers fueled privacy concerns, spawning a series of industry reforms. For example, the 2014 hacking of Target's payment card system spurred U.S. card networks, card issuers, and retailers to begin implementing the use of EMV chip cards, a transition that is still underway.

Ransomware attacks, targeted breaches of health information, and foreign government involvement in cybersecurity attacks have emerged as common features of the security landscape in 2016. A recent distributed denial of service (DDoS) attack affecting major social media sites was attributed to security vulnerabilities in Chinese-made connected devices and has kept attention on the vulnerabilities of connected products.[12]

Children have always imagined that their toys could understand and talk back to them. Now, they actually can. These new play experiences come with the same potential pitfalls and threats that general audience products do, but with vulnerable children, companies are expected to take special precautions. Unfortunately, although headlines about connected toy privacy and security perils are often either exaggerated or simply untrue, we expect that advocates will continue to highlight connected toys as part of a broader privacy and anti-advertising agenda.

With a decade of technological tumult behind us, 2017 promises a continued rollercoaster. The new Trump Administration in Washington has upended expectations about how the U.S. government will address privacy and security even as the European Union marches toward the May 2018 entry into force of the GDPR. "America First" rhetoric coming from the White House may further complicate the ability to negotiate on a variety of issues with other countries, including agreements touching on privacy and security. Against these uncertainties, toymakers must continue to innovate, recognizing that even if government enforcement initiatives slow down, connected toys and children's products will remain a lightning rod. It is more important than ever for manufacturers to also increase their focus on privacy and security as they develop new connected toys.

---

[11] *See* Brian Krebs, *Yahoo: One Billion More Accounts Hacked*, Krebs on Security (Dec. 14, 2016), *available at* http://bit.ly/2hvuyKT.

[12] *See* Alexander J. Martin, *Chinese electronics biz recalls webcams at heart of botnet DDoS woes: US products compromised by Mirai mischief in another Internet of Things success*, The Register (Oct. 24, 2016), http://bit.ly/2dTyx2L.

II. Upending Expectations: An Era of GOP Control Dawns

Newly minted Republican control of all branches of government in Washington means uncertainty in consumer privacy and data security priorities and enforcement. It also means a complicated relationship with how privacy rights are balanced with national security interests, which could have far-reaching implications with trading partners whose privacy regimes favor personal privacy rights. While in the short-term the anticipated threat of possible new U.S. privacy or security legislation or new regulations seems to have waned, we still expect to see the FTC acting as the chief privacy and security enforcement arm in the U.S., although application of enforcement policies could be more business-friendly. If enforcement dramatically tails off, however, a vacuum in federal consumer protection activity could result in much more state legislation, attorney general (AG) enforcement actions, and class action litigation.

A. The White House, FTC, and Other Agencies

1. The White House

The Obama Administration viewed privacy as a key issue, but failed to persuade the Republican-dominated Congress to enact its proposed Consumer Bill of Rights in 2012 and again in 2015.[13] Former President Obama also promoted a variety of initiatives on cybersecurity. There is no indication that President Trump supports an overall privacy measure, and his reluctant recognition of a Russian role in attempting to influence the election was coupled with assertions that the hacking was primarily due to weak security by the Democratic National Committee (DNC). It remains unclear how the new President will approach the threat of foreign government interference in cyberspace or data security standards for U.S. government and private entities.

Some administrative priorities may spill over into the realm of privacy and security. For example, in the early days of his administration, President Trump signed an executive order "direct[ing] executive departments and agencies to employ all lawful means to enforce the immigration laws of the United States." This order included a provision directing them to "ensure that their privacy policies exclude … [non-U.S. citizens or lawful permanent residents] from the protections of the Privacy

[13] *See* Executive Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), available at https://www.whitehouse.gov/sites/default/files/privacy-final.pdf; Office of Management & Budget, *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015* (Feb. 27, 2015), available at http://bit.ly/1MV202Y.

Act regarding personally identifiable information."[14] Given that Congress had recently adopted a law extending Privacy Act protections to European Union citizens to ensure data flows between Europe and the U.S.,[15] showing rare bipartisan support, some commenters asked whether this would impede those data flows and inquired about the role of Congress in enacting that legislation.[16] Later interpretation by the European Commission clarified that the Commission did not consider the order to limit those protections in the context of the law.[17] Although confusion on this particular point seems to have lifted, at least for now, the episode illustrates how the Trump Administration's efforts to implement sweeping campaign promises to halt immigration and secure the borders create uncertainty affecting how businesses manage global data transfers to meet the requirements of European law.

2. FTC and FCC

The FTC has been the U.S. privacy enforcement watchdog, a role that seems likely to continue given its broad powers. Under Section 5 of the FTC Act, the Commission has the authority to take action against unfair and deceptive business practices[18] and also has specific enforcement jurisdiction under COPPA and a variety of other laws to deal with sector-specific aspects of privacy.

In the privacy and security arena, The FTC has initiated privacy enforcement actions based on a firm's failure to abide by promises in its privacy policy and terms of service. The FTC has also expanded application of its unfairness authority in security cases, arguing that lax or unmaintained security is an "unfair" practice under Section 5.

The underlying principles of Section 5 will likely continue to guide the FTC's assessments, inquiries, and prosecutorial targets in the Trump Administration on all consumer protection issues under FTC jurisdiction. However, the FTC's expanded interpretation of its unfairness authority in two recent security breach

---

[14] *See* E.O. 13,768 §§ 1 & 14, 82 Fed. Reg. _ (to be published Jan. 30, 2017).

[15] *See* n. 35 *below and associated text.*

[16] *See, for example*, Jan Philipp Albrecht, Tweet of Jan. 26, 2017 at 4:45 a.m. (ET), Twitter, https://twitter.com/JanAlbrecht/status/824553962678390784 (last accessed Jan. 27, 2017).

[17] *See* Natasha Lomas, *Trump order strips privacy rights from non-U.S. citizens, could nix EU–US data flows*, http://tcrn.ch/2kxo7IY (Jan. 26, 2017, last accessed Jan. 27, 2017, at 12:27 p.m.) (quoting statement from Commission that the U.S.–EU Privacy Shield "does not rely on the protections under the U.S. Privacy Act").

[18] 15 U.S.C. § 45.

cases, *FTC v. Wyndham Worldwide Corp.*[19] and *In re LabMD, Inc.*[20] garnered serious criticism and that interpretation is likely to be rolled back. In fact, the agency's own administrative law judge (ALJ) in the *LabMD* case found that the evidence FTC staff submitted amounted only to "hypothetical or theoretical harm," insufficient to meet the standard of proof under the FTC Act. ALJ rulings can be appealed to the full Commission. Not surprising, a majority at the Commission reversed the decision, finding that the mere disclosure of sensitive medical information is a cognizable harm under FTC Act § 5(c).[21] Although the FTC overruled the ALJ, the case continues after LabMD obtained new representation and appealed the FTC's decision to the Eleventh Circuit Court of Appeals.

President Trump has not spoken on consumer protection issues, but has, rather surprisingly, quickly named Republican Commissioner Maureen Ohlhausen acting chair of the FTC.[22] Former Commissioner Joshua Wright is aiding the Trump transition team on FTC issues, and is another possible nominee as permanent chair. Some signals about a Republican-controlled FTC's approach in 2017 and beyond may be gleaned from then-Commissioner Ohlhausen's votes and statements on privacy and data security during the Obama years.

Ohlhausen agreed with President Obama on underlying principles of privacy, including privacy by design, simplified notice and choice options for businesses and consumers, and transparent disclosure of the collection and use of consumers' information.[23] However, she opposed the settlement with reputation management company LifeLock, Inc. Rather than rejecting the FTC's theory that failure to offer information security is unfair, she instead argued that the record lacked "clear and convincing evidence that LifeLock failed to establish and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of consumers' personal information." She further noted that there was no evidence that "LifeLock subscribers' information suffered a breach."[24] Most recently, then-Commissioner Ohlhausen voted against issuing a complaint about D-

---

[19] 799 F.3d 236 (3d Cir. 2015).

[20] FTC No. 9357 (filed Aug. 29, 2013).

[21] *See* Op. & Final Order, *id.* (July 29, 2016), *available at* http://bit.ly/2ha2Or7.

[22] *See* FTC, *Statement of Acting FTC Chairman Maureen K. Olhausen on Appointment by President Trump* (Jan. 25, 2017), *available at* http://bit.ly/2k1oquv.

[23] *See* Remarks of Commissioner Maureen K. Ohlhausen, *NAI Summit: Third Parties and the Future of the Internet* *2–*3 (May 21, 2013), *available at* http://bit.ly/2hzfRmT.

[24] *See* Dissenting Statement of Commissioner Maureen K. Ohlhausen, *FTC v. LifeLock, Inc.*, Matter X100023 (Dec. 17, 2015), *available at* http://bit.ly/2iaeOKW.

Link's security practices.[25] D-Link has aggressive defended itself, and this case may be the first test of whether the FTC will proceed with an enforcement action absent an actual breach that results in harm to affected consumers.

The FTC has been less subject to political changes affecting its enforcement mission than other agencies. No evidence of harm is needed where violations of COPPA or specific statues are concerned, but if the FTC staff shifts toward Acting Chairman Ohlhausen's views, as we expect is likely, toymakers and others can expect that the FTC's general security enforcement actions will focus on cases involving *actual* and *demonstrated* harm to consumers. And, of course, it is likely that the FTC will to continue to hold workshops and other events to help the agency understand the changing technology landscape and implications for privacy and security, and will continue to offer general guidance on what it considers to be "best practices."

The Federal Communications Commission (FCC) also pursued an aggressive privacy regulatory agenda under the Obama Administration, finalizing a far-reaching privacy rule governing broadband and cellular service providers (ISPs). One key element of the FCC rule is a broad definition of "personal information" that encompasses IP addresses and device identifiers. Republican Commissioner Ajit Pai has been named acting chair of the FCC, and is expected to work to reverse the rule. Even if the rule is revoked, given the broad EU definition of "personal" information, federal definitions may matter less and less for global marketers.

3. DOC

While the major developments at the U.S. Department of Commerce (DOC) have been the negotiation of the EU-U.S. Privacy Shield[26] and recent U.S.-Swiss Privacy Shield[27] discussed later, DOC's National Telecommunications and Information Administration (NTIA) has also been active. NTIA initiated multi-stakeholder initiatives on privacy and just released an IoT green paper, soliciting additional comments on its role in fostering the IoT.

With respect to privacy, NTIA's multi-stakeholder initiatives have focused on privacy considerations associated with apps, facial recognition technology and unmanned aircraft systems (drones). NTIA's recommended best practices on facial

---

[25] See FTC, *FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras* (Jan. 5, 2017), available at http://bit.ly/2ihW6o4.

[26] *See, for example,* U.S. International Trade Administration, *Notice of Availability of Privacy Shield Framework Documents*, 81 Fed. Reg. 51,041 (Aug. 2, 2016).

[27] *See* (Swiss) Federal Data Protection and Information Commissioner, *Swiss–US Privacy Shield: new framework for the transfer of data to the USA* (Jan. 11, 2017), *available at* http://bit.ly/2iFICxT.

recognition technology include transparent policies and disclosures, the development of good management practices, use limitations, and appropriate security safeguards, among other considerations.[28] Drone best practice recommendations are analogous, covering the need to inform others of the use of drones; showing care in operating drones and collecting or storing data through them; limiting the use and sharing of certain types of data; and securing such data.[29] Both build on the first of the NTIA multi-stakeholder codes for mobile apps.[30] While industry has participated in the NTIA initiatives, industry sectors have not endorsed the codes and companies have not pledged compliance, largely because violations could constitute and unfair and deceptive acts or practices enforceable by the FTC.

The IoT green paper lays out an approach and areas of engagement for the NTIA to pursue in the future.[31] It speaks to the broad benefits of IoT technologies and stresses the importance of growing the digital economy and spurring innovation. The green paper then outlines a number of key principles that should underpin NTIA's work. These include ensuring that the IoT environment is inclusive and widely accessible; stable, secure and trustworthy; and globally connected, open and interoperable. NTIA is seeking public comments on the green paper. Ultimately the principles outlined could guide future NTIA and other government actions and initiatives on aspects of IoT and the digital economy generally.

B. Congress

Allegations that the DNC and emails associated with Hillary Clinton and some of her associates were hacked by Russia, influencing the 2016 presidential campaign, continue to swirl and appear headed for at least one major Congressional investigation into foreign snooping. At the time of this writing, both the CIA and FBI agreed that Russian hackers intended to affect the 2016 presidential result, leading President Obama to announce sanctions. President Trump, who initially scoffed at the allegations, acknowledged Russian involvement while insisting that it did not change the election outcome. Key Republican figures in Congress

---

[28] *See* NTIA Privacy Multistakeholder Process: Facial Recognition Technology, *Privacy Best Practice Recommendations for Commercial Facial Recognition Use* (June 15, 2016), *available at* http://bit.ly/2k2SmY5.

[29] See NTIA, *NTIA Multistakeholder Process: Unmanned Aircraft Systems, Voluntary Best Practices for UAS Privacy, Transparency, and Accountability: Consensus, Stakeholder-Drafted Best Practices Created in the NTIA-Convened Multistakeholder Process* (May 18, 2016, updated June 21, 2016), available at http://bit.ly/2ekuVoP.

[30] *See* NTIA, *Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices* (July 25, 2013), *available at* http://bit.ly/2jQs8qU.

[31] *See* NTIA, *Fostering the Advancement of the Internet of Things* (Jan. 12, 2017), *available at* http://bit.ly/2jwM0iC.

nevertheless have expressed steady concern about Russian interference and support for hearings, and there will likely be increased pressure to bulk up U.S. cybersecurity universally.

The Bipartisan Congressional Privacy Caucus continues to be one of the largest. Both Democrats and Republicans have been involved in hearings and inquiries related to alleged breaches of consumer information. Moreover, in late 2015 and into 2016, allegations about security vulnerabilities of connected toys prompted multiple investigations, spearheaded by Democratic Senators Ben Nelson (D-FL) and Al Franken (D-MN), and urged by privacy NGOs in 2016.

In fact, as the capstone of his investigation, in December 2016, amid the holiday toy buying season, Senator Nelson released a report focused on his findings regarding alleged security vulnerabilities of connected toys that could have compromised the private information of children or their parents.[32] The report singled out three manufacturers, although only one of the companies actually suffered a breach. The report acknowledged that of the remaining two, one manufacturer fixed the potential vulnerability in a week; the other in four hours. The report, underway for many months, was developed with expectations that Hillary Clinton would become president and would be receptive to more privacy legislation. In the current environment, however, the report received little public attention.

The changed political landscape and continued polarization on the Hill, however, actually may increase the likelihood that advocates will seek to politicize allegations that toy companies are violating children's privacy. Thus, we not only expect to see proposed legislation on children's and student privacy introduced in this Congress, we anticipate that key Democrats will actively keep the spotlight on children's advertising and privacy. Versions of the Do Not Track Kids Act, which would ban tracking of children and expand privacy protections for teens, were proposed in 2011, 2013, and 2015, for example, and garnered some bipartisan support.[33] Similarly, members of both houses have sponsored and proposed student privacy bills that would prohibit pre-, elementary, and secondary schools' ISPs and online service providers from using targeted OBA or ads based on PII.[34] Still, with

---

[32] *See* U.S. Senate Committee on Commerce, Science & Transportation, Office of Oversight & Investigations, Minority Staff Report, *Children's Connected Toys: Data Security & Privacy Concerns* (Dec. 14, 2016), *available at* http://bit.ly/2hzuTJf.

[33] Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011); Do Not Track Kids Act of 2013, S. 1700 & H.R. 3481, 113th Cong. (2013); Do Not Track Kids Act of 2015 S. 1563 & H.R. 2734 (2015).

[34] *See* Safeguarding American Families from Exposure by Keeping Information and Data Secure (SAFE KIDS) Act, S. 1788 (2015); Student Digital Privacy and Parental Rights Act of 2015, H.R. 2092 (2015).

vows from the President-elect to roll back regulation, the prospect of enacting legislation imposing broad new requirements on businesses is low at present.

Trade implications of privacy, on the other hand, did result in quick bipartisan legislative action last year when Congress approved the Judicial Redress Act (JRA) as part of the effort to maintain an alternative method to assure that data transfers from the EU to the U.S. meet EU adequacy requirements. The JRA grants an unusual private right of action to Europeans whose privacy rights are violated by U.S. actors. The law was adopted as part of the compromise that resulted in the EU–U.S. Privacy Shield, the data transfer instrument that replaced the U.S.–EU Safe Harbor struck down by the European Court of Justice in late 2015 (discussed later in this paper). The Act's approval in the 114th Congress[35] – a Congress not known for passing many substantive bills – points to the importance of ensuring that transatlantic data flows continue with few to no impediments. As noted earlier, however, President Trump's executive orders and pronouncements may further complicate the global data flow landscape.

C. States

States have led the way in adopting legislation to safeguard privacy and security. California, for example, requires websites to tell consumers about disclosure of personal information to third parties who use that information for direct marketing purposes.[36] California also requires data breaches to be reported via the state's online portal,[37] and posts breach notices on the California AG's website. Indeed, data breach notification requirements exist in all but two states, and state-specific requirements and forms complicate the task of sending breach notices to consumers.

Even during a period where the Obama Administration actively enforced privacy and security lapses, state legislative activity levels were moderately high. If the federal government is seen to be lax in enforcing privacy and security protections for consumers, state activity is likely to increase further, and state enforcement actions could increase. There are a variety of private rights of action that state attorneys general have invoked using their general consumer protection or false advertising authority, or, in specific cases, applying the doctrine of *parens patriae* to assert violations of federal statutes such as COPPA on behalf of their citizens. The

---

[35] *See* Judicial Redress Act of 2015, Pub. L. 114–126, 130 Stat. 282 (Feb. 24, 2016).

[36] *See* Cal. Bus. & Prof. Code §§ 22575–22579.

[37] *See* Cal. Civ. Code § 1798.82(a), (f); Office of the (California) Attorney General, *Search Data Security Breaches* (last updated Dec. 22, 2016), https://oag.ca.gov/ecrime/databreach/list.

attorneys general of New York,[38] New Jersey,[39] and Texas[40] have each brought COPPA enforcement actions. If the FTC is seen as less aggressive in advancing the consumer agenda on privacy and security, more such cases can be expected.

D. NGOs

NGOs have been harsh critics of kid-directed apps, websites, and connected toys. Groups opposed to marketing to children are joining with privacy organizations, regularly filing petitions to the FTC to investigate alleged vulnerabilities. Interestingly, although the FTC investigates petitions in response, few, if any, consent agreements have resulted from them. FTC investigations are non-public. If the FTC concludes no action is warranted, there is typically no further word on the topic and the FTC does not generally issue a closing letter. Instead, over time, the absence of any announced action from the FTC can generally be viewed as an indication that the FTC concluded that no violation occurred. Petitions, however, also tend to prompt congressional interest or a consumer response, and generally are associated with social media initiatives asking consumers to support an inquiry, halt purchases of the product, or take other action.

The most recent NGO tactic involved filing cross-border petitions alleging privacy and advertising violations by Genesis Toys in connection with two of the company's connected toys. On December 6, 2016, several NGOs in the U.S. (including the Electronic Privacy Information Center, the Campaign for a Commercial Free Childhood, the Center for Digital Democracy, and the Consumers Union) filed a petition with the FTC[41] alleging privacy and security issues with two connected toys. Simultaneously, *Forbrukerrådat*, the Norwegian Consumer Council,

---

[38] See Office of the (New York) Attorney General, *A.G. Schneiderman Announces Results of "Operation Child Tracker," Ending Illegal Online Tracking of Children at Some of Nation's Most Popular Kids' Websites* (Sep. 13, 2016), available at http://on.ny.gov/2c8jAJd.

[39] *See, for example, In the Matter of Dokogeo, Inc.* (N.J. Dep't of Law & Pub. Safety, Div. of Consumer Affs. Nov. 13, 2013), http://nj.gov/oag/newsreleases13/Dokogeo-Inc_&_Dokobots.pdf; *In the Matter of Dokogeo, Inc.* ¶ 5.1 (N.J. Dep't of Law & Pub. Safety, Div. of Consumer Affs. Nov. 13, 2013), http://nj.gov/oag/newsreleases13/Dokogeo-Inc_&_Dokobots.pdf.

[40] *See* Assurance of Voluntary Compliance, *In re State of Texas and Juxta Labs*, Case No. D-1-GN-16-004940 (D. Ct., Travis Cty., Tex., filed Sep. 30, 2016), *available at* http://bit.ly/2i8TQw9.

[41] *See* EPIC, *et al.*, *Complaint, In re Genesis Toys and Nuance Communications* (FTC, filed Dec. 6, 2016), *available at* http://bit.ly/2gNpdOb.

spearheaded an effort by a coalition of consumer groups in filing petitions with the Norwegian DPA[42] and the EC.[43]

Both sets of petitions concerned alleged "spying" by two connected toys, Cayla and the i-Que robot. Notably, background documents indicate that other products, such as Hello Barbie, were investigated but the groups did *not* find security vulnerabilities in the product.[44] The EU petition and report were accompanied by a video depicting alleged security weaknesses, including the range at which Bluetooth connected toys could "overhear" other conversations. One of the targeted products was subsequently removed from the shelves by major retailer Toys R Us, and other retailers were pressured to do the same.[45] The action prompted a discussion of whether data security obligations should be incorporated into the European toy safety requirements in the EU.

E. Plaintiffs' Lawyers

Plaintiffs' lawyers, especially class action lawyers, are also major players in the privacy and security space and pay special attention to the wording of company privacy policies. Facebook, for example, has faced down plaintiffs' lawyers on multiple occasions over its privacy policy, particularly in California.[46] Often these suits seek to bootstrap alleged regulatory violations but face procedural hurdles in doing so.

In one important case, *Spokeo, Inc. v. Robins,* the plaintiff alleged that inaccurate information published by Spokeo (a "people search engine") entitled him to damages under the Fair Credit Reporting Act (FCRA). The Supreme Court held that "Robins [could not] satisfy the demands of Article III by alleging a bare procedural violation." The Court remanded the case to the Ninth Circuit Court of Appeals to consider "whether the particular procedural violations alleged in this case entail a degree of risk sufficient to meet the concreteness requirement" of Article III standing requirements.[47]

---

[42] See Forbrukerrådat, *Complaint regarding user agreements and privacy policies for internet-connected toys – the Cayla doll and i-Que robot* (Dec. 6, 2016), *available at* http://bit.ly/2i1kWYh.

[43] See BEUC, *Consumer organisations across the EU take action against flawed internet-connected toys* (Dec. 6, 2016), *available at* http://bit.ly/2g5Rf8q.

[44] *See* Bouvet, *Report: Investigation of privacy and security issues with smart toys* (Nov. 11, 2016), *available at* http://bit.ly/2kgaGtR.

[45] *See How "smart devices" that listen to you could compromise your privacy*, CBS News (Dec 21, 2016), *available at* http://cbsn.ws/2i1pjzN.

[46] *See, for example, Fraley v. Facebook, Inc.*, Case No. 11-CV-01726 (N.D. Cal., filed Apr. 4, 2011).

[47] *See Spokeo, Inc. v. Robins*, Case 13–1339, __ U.S. __, 136 S. Ct. 1,540 (decided May 16, 2016), *available at* http://bit.ly/2iyw37Y.

Procedural violations that give rise to "particularized" harms but not the necessary "concrete" harm are more likely to be dismissed by the courts, and privacy claims often fail this test. Courts have limited class actions in numerous cases since *Spokeo*, suggesting that consumers will face higher hurdles in moving cases forward absent evidence of damages. To the extent the FTC moves to establish a harms-based standard in security cases, this could affect judicial thinking on the topic as well.

III. Europe Drives Global Privacy Policies

European privacy developments, however, are likely to become even more influential in global policy and business practice. In Europe, privacy is regarded as a fundamental human right. This is perhaps the most important reason for the muscular approach taken by EU and national authorities in developing and enforcing privacy laws. Europe, unsurprisingly, reacted with outrage to Snowden's revelation of international tracking by the national security agency. European regulators also seem to focus heavily on U.S. businesses when enforcing privacy laws.

At the same time, however, the increase in terrorist attacks on European soil has resulted in concomitant efforts to increase government surveillance tools to keep citizens safe. The prospect of such attacks does not seem to be declining, and that reality may increase discussions about how to balance privacy rights with national security concerns in Europe. The result of competing security/privacy interests may be to ratchet up restrictions on data collection associated with marketing activities, especially where children are concerned, even as governments gain or exercise new and broader monitoring powers. At present, the growing populist movement in Europe has not appeared to affect how many European citizens view privacy, but the growth of nationalism may also affect how different countries weigh the balance of security and privacy policy objectives.

A. ECJ Drives Dramatic Changes

1. The "Right to Be Forgotten"

European law and court decisions also continue to be enormously influential in the global privacy landscape. In a landmark 2014 case, a Spanish lawyer sued Google after a search for his name on the search engine turned up accurate, but somewhat dated, legal notices related to his debts and information on the forced sale of his property, originally published in an online Spanish newspaper. The Spanish Data Protection Agency ruled against Google but did not require the newspaper to remove the data. Google appealed to the European Court of Justice (ECJ), which held that under certain circumstances Google must delete the personal data of

Europeans from search results at a user's request.[48] Google has reportedly received hundreds of thousands of requests related to this so-called "right to be forgotten."

The scope of the right to be forgotten continues to ensnare Google in new legal challenges. The French DPA, *Commission Nationale de l'Informatique et des Libertés*, or CNIL, fined Alphabet's Google €100,000 over the alleged failure to properly process requests from French citizens to delete their data from search results. Although Google removed links to the requestor's information on the search engine's European geographic domains (for example, google.fr), the information remained accessible on .com and other non-European domains.[49] Google plans to appeal the ruling.

In the U.S., courts are not likely to elevate privacy rights over speech rights absent special circumstances. Truthful but old information about the bankruptcy of an attorney may still be relevant to individuals looking for legal representation, for example. The right to be forgotten controversy, however, illustrates tensions between First Amendment rights in the U.S. to know, hear, and speak, and the concept of privacy as a fundamental human right in the EU. Those tensions are likely to be magnified when the GDPR goes into effect. How those will play out, and implications of the GDPR's purported extraterritorial reach, are certain to be heard in various courts.

2. The Schrems Decision and Impact on Adequacy of Data Transfer Mechanisms

The right to be forgotten is not the only area where EU and U.S. approaches to privacy differ. EU law restricts transfers of data to countries that lack an "adequate" regime of privacy, which has resulted in the development of some specific mechanisms under which data can be transferred. These include binding corporate rules, approved contracts, and the U.S.–EU Safe Harbor Framework.

The Safe Harbor, negotiated between the U.S. Department of Commerce (DOC) and the European Commission (EC) in 2000, allowed data transfers between the U.S. and EU so long as the U.S. entity comported with seven privacy principles. Companies that registered with DOC were generally protected from inquiries by EU Member States' data protection authorities (DPAs). Safe Harbor-registered entities were required to self-certify that they took adequate precautions to protect data.

---

[48] *See Google Spain SL v. Agencia Española de Protección de Datos*, ECJ Case C-131/12 (May 13, 2014), *available at* http://bit.ly/2haCzkf.

[49] *See* CNIL, *Right to be delisted: the CNIL Restricted Committee imposes a €100,000 fine on Google* (Mar. 24, 2016), http://bit.ly/2ioJQOq; *see also* Decision on a financial penalty for Google, CNIL 2016–054 (Mar. 10, 2016).

Failing to abide by the certification constituted misrepresentation, subjecting them to potential civil liability.

The Framework, viewed as an important, convenient mechanism to meet adequacy requirements, was threatened when Austrian law student Max Schrems challenged Facebook's compliance with EU data privacy laws in 2013.[50] Schrems claimed that the Safe Harbor Framework fails to guarantee adequate protection of EU citizen data based on evidence from Snowden and WikiLeaks about the U.S. National Security Agency's (NSA) surveillance activities. Although the Irish DPA rejected his claim, Schrems appealed and the case was referred to the ECJ, which ruled that the Safe Harbor Framework was inadequate to ensure compliance with the privacy principles. Importantly, the ECJ concluded that DPAs could independently evaluate whether EU citizens' right to privacy would be protected by the Safe Harbor.

Subsequently, after intense negotiations, the European Commission and DOC reached agreement on an instrument to replace the Safe Harbor. The new EU–U.S. Privacy Shield includes several critical elements:

- companies handling employee data must commit to comply with European DPAs' decisions;
- U.S. law enforcement and national security access to EU citizens' personal data will be the exception, and "must be used only to the extent necessary and proportionate";
- annual joint review of this arrangement will be held; and
- European citizens will have redress for alleged misuse of their data through new obligations of companies to respond to complaints through no-charge alternative dispute resolution and other routes.

As of this writing, more than 1,300 companies have registered with DOC as Privacy Shield participants.[51]

Key to approval of the Privacy Shield was the Judicial Redress Act, which extends the primary rights U.S. citizens enjoy under the Privacy Act to European citizens. EU citizens will be able to file suit in the U.S. for improperly disclosed personal information gathered in connection with international law enforcement

[50] *Schrems v. (Irish) Data Protection Commissioner*, ECJ C-362/14.

[51] *See* International Trade Administration, *Privacy Shield Framework: Privacy Shield List* (last accessed Dec. 26, 2016), *available at* http://bit.ly/2b0Ijdq.

efforts.[52] The U.S. also just completed a similar agreement with Switzerland,[53] which offers U.S. companies the opportunity to transfer data on Swiss citizens to the U.S. under the same framework as the EU–U.S. Privacy Shield (upon appropriate determination of the U.S. Attorney General, Swiss citizens would be able to bring actions against U.S. agencies under the Privacy Act). While the adoption of the Privacy Shield continues to enable data transfers to occur between the U.S. and Europe, the increased number of procedures and specific protections for EU data subjects may make the system more difficult to comply with than under the Safe Harbor framework. These complications are likely to grow following implementation of the new GDPR. Those complexities will be exacerbated by White House pronouncements that create uncertainties about the validity of the previously negotiated framework.

B. GDPR

The GDPR, which becomes effective in May 2018, consolidates and modifies the framework of European privacy law, replacing the Data Protection Directive. While the enforcement deadline is fast approaching, there are substantial uncertainties as the authorities, including the European Commission and the DPAs (in the guise of the current Article 29 Working Party), have only just begun to issue guidance documents to flesh out the details of how the GDPR will work.

1. The Framework

The reforms will give European consumers new rights and controls over their personal information. They will impose new obligations on businesses that collect personal information from EU citizens, regardless of where they reside, and on individuals who reside in the EU, regardless of their nationality. The new rules empower individuals by, among other things, (1) providing easier access to personal data and more information on how data is processed; (2) facilitating data portability or transfers of personal data between service providers; (3) clarifying the right to be forgotten for individuals who no longer wish for their data to be processed; and (4) requiring expedited notifications to the national supervisory authority by companies that experience a data breach affecting personal data.

While some of the new measures are intended to make the system less cumbersome, the broad reach, new restrictions, expanded obligations, and enhanced penalties imposed on businesses could more than offset these reductions. Given the

---

[52] *See* Privacy Act of 1974, Pub. L. 93–579, 88 Stat. 1,896 (Dec. 31, 1974), *codified at* 5 U.S.C. § 552a.

[53] *See* (Swiss) Federal Council, *Swiss–US Privacy Shield: better protection for data transferred to the USA* (Jan. 11, 2017), *available at* http://bit.ly/2j5N90p.

magnitude of new requirements in the GDPR, it will be important for companies to begin the compliance process now.

2. Article 29 Working Party Starts Issuing GDPR Guidance

In December 2016, the Article 29 Working Party addressed certain questions arising under the GDPR. Specifically, the Working Party explained that an entity's Data Protection Officer (DPO) would not be held liable for failure to properly manage personal data, as liability is assigned to the data processor or controller.[54] The Working Party also released guidance on data portability,[55] explaining the conditions under which this new right applies, taking into account the fact that this right is limited to data provided by an EU citizen. It recommended starting the process to develop appropriate responses to data portability requests, including development of download tools and application programming interfaces (APIs). Finally, the Working Party issued its guidelines on the Lead Supervisory Authority (LSA),[56] explaining particular terms and concepts incorporated in the relevant GDPR provisions. For example, correct identification of controllers' location of "central administration" will guide the determination of the LSA. The guidelines are open for public comment until January 2017.

The Working Party expects to address additional information topics in guidance documents in 2017, including the consent, individual profiling, and transparency provisions of the GDPR, as well as privacy certification, high-risk data processing, administrative fines, and the organization and functioning of the new European Data Protection Board (which will replace the Working Party once the GDPR takes effect). However, guidance on the specific scope of obligations related to children's privacy has not been included in the list of topics.

3. Open Questions

One of the most important open GDPR implementation questions for toy companies is the scope of privacy protection for children. For example, the GDPR defines children to include those up to 16 years old, but it allows Member States to

---

[54] *See* Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs')*, 16/EN WP 243 (Dec. 13, 2016), *available at* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf.

[55] *See* Article 29 Working Party, *Guidelines on the right to data portability*, 16/EN WP 242 (Dec. 13, 2016), *available at* http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf.

[56] *See* Article 29 Working Party, *Guidelines for identifying a controller or processor's lead supervisory authority*, 16/EN WP 244 (Dec. 13, 2016), http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf.

set a lower age as long as it is not less than 13 years old. This creates major uncertainties for marketers who have relied on the age-13 cut-off in developing internationally-accessible websites and apps.

The International Chamber of Commerce (ICC) recently released a statement of code interpretation on age considerations for marketing to children and teens. The ICC, while recognizing that such definitions are often a matter for national law, takes the view that "children" are those aged 12 and under, and that "teenagers" are those aged 13 to 18.[57] (Teenagers should not be treated like children for advertising or privacy purposes.) However "children" are ultimately defined, it remains unclear whether guidance from the authorities will mirror approaches to and exemptions from parental consent obligations under COPPA when it comes to children's privacy. Moreover, although data collection may take place where the legitimate interest of the controller outweighs the fundamental privacy interests of the data subject (including a child), some assert that where children are concerned, the only proper legal basis for processing data is with the consent of a parent. If this is the case, it could force a sea change in how toy companies must structure websites, apps, and other services. To obtain consent, they may have to block child visitors until a parent registers. This could mean that toy companies could not offer the type of anonymous registration that rests on collecting a first name or user name and password from a child, and may well decide to collect far more information initially from parents.

Other important EU developments potentially affecting privacy and security requirements involve the review of the E-Privacy Directive[58] and the revision of the Audiovisual Media Services Directive (AVMSD).[59] The former is commonly known as the "cookie" directive, and under it the EU imposes strict limits on use of cookies absent consent. Indications are that this approach will be extended to non-cookie technologies as well. A recently released proposed replacement for the E-Privacy Directive aims to simplify some aspects of cookie consent (for example, through browser settings) and eliminate the need for consent for "non-privacy intrusive cookies" such as those used to remember shopping cart history.[60] This could include the types of cookies used to recognize an anonymous returning visitor who has registered with a user name and password.

---

[57] *See* International Chamber of Commerce, *ICC Statement on Code Interpretation: ICC Reference Guide on Advertising to Children* (Dec. 14, 2016), *available at* http://bit.ly/2hkKrzu.

[58] Directive 2002/58/EC (July 12, 2002).

[59] Directive 2010/13/EU (April 15, 2010).

[60] *See* EC, *Proposal for a Regulation of the European Parliament and of the Council to Replace Directive 2002/58/EC*, COM(2017) 10 final (2017/0003 (COD)) (Jan. 10, 2017), *available at* http://bit.ly/2jhSq2z.

The GDPR now establishes that if a child under 16 (or other national age no lower than age 13) is involved, consent must come from a parent. How these two instruments will connect is an open question. If, as is currently the case, consent is required for use of all cookies (or other technologies) that are not "strictly necessary" to operate the website, operational and practical questions will abound, and those operational difficulties will be exacerbated if EU authorities determine that consent is the only legal basis under which data from children can be processed.

While not directly implicating privacy, another critically important development in the EU is the update of the AVMSD. The AVMSD sets out principles for a safe, pluralistic, and open audiovisual media landscape within the EU, including content provisions. These include requirements that commercial communications be clearly identifiable as such, limitations on "hate" or discriminatory communications, and accessibility provisions. The revision under consideration[61] would address new developments, such as the prominence of streaming services such as Netflix, but the proposed revision's undertones appear relatively hostile to advertising. More worrisome still is that the amendment process could entirely ban commercial communications to all minors, in not just broadcast but all media. With some activists asserting that "commercial communications" should be broadly defined, restrictions could affect the type of branded entertainment that is increasingly a hallmark.

In addition to the GDPR, the E-Privacy Directive, and the update to the AVMSD, changes to the Unfair Commercial Practices Directive[62] are also likely after the EC released a report identifying "detriment and lost opportunities for consumers, in sectors where the Single Market's growth potential is the highest, such as travel and transport, digital and on-line, financial services and immovable property."[63] The changes are part of a larger EC "fitness check" regarding commercial and marketing regulations, so it is important to keep an eye on international policy developments.

---

[61] *See* EC, *Proposal for a Directive of the European Parliament and of the Council to Replace Directive 2010/13/EU*, COM(2016) 287 final (2016/0151 (COD)) (May 25, 2016), *available at* http://bit.ly/2fEjR3H.

[62] Directive 2005/29/EC (May 11, 2005).

[63] *See* EC, *Unfair commercial practices directive* (n.d.), *available at* http://bit.ly/2kfX1To.

IV. Conclusion

A. Compliance Frameworks

1. General Preparations

Preparing for and ensuring continuing compliance with any privacy or data security law or best practices starts with mapping the data collected, then conducting internal and external assessments to evaluate whether the steps and systems currently implemented are sufficient to comply with the requirements, and to address known and potential cyber threats to collected data. These assessments can help companies determine whether they are keeping up with industry best practices, and can serve to defend against regulatory investigations and lawsuits. While that remains an important and necessary initial step in the GDPR compliance process, identifying gaps in procedures and implementing compliance programs is complicated by the current lack of guidance.

Whether the application of the GDPR's new provisions on children's privacy will track closely with COPPA is yet unknown. While COPPA does impose a strict liability standard on data collection by third parties on child-directed websites, apps, and services, and requires due care in maintaining security, the standard is reasonable, not unfailing, security. The most technically adept companies in the world do not expect the code that they ship to be error-free; this includes major software publishers like Apple, Microsoft, Google, and Oracle. Instead, these businesses test and fix bugs before shipping (including extensive, sometimes public, beta testing). They then continue to accept reports from individuals and third parties on additional issues and offer software updates to plug vulnerabilities. However, it seems likely that societal expectations for toy company privacy and security practices will be very high. Toy companies will be expected to understand and adhere to best practices, continually work on improvement, and address problems promptly when they are identified. This also requires strategy for patching and updating privacy and security-related software, particularly for connected toys, as well as disclosures about whether updates will cease at some point.

2. Steps for Complying with the GDPR

Because most toy companies operate internationally, they will be subject to the GDPR. Most companies operate with multiple streams of data, such as human resources data, consumer data, vendor/supplier data, etc. Mapping these data flows, creating the relevant compliance structures and processes to cover the different categories of data, and documenting them will rapidly consume the year and a half remaining before the GDPR becomes mandatory. Normally, a good starting point is for businesses to assess their current practices, identify gaps, and use that

information in a data mapping exercise to line out a step-by-step compliance plan. However, because the full contours of how the new GDPR will apply to children's data may not be fully clear until 2018, the normal timelines for the exercise could be compressed. Nevertheless, such exercises will be crucial to assess global data flows and related compliance obligations.

3. Preparing for Legislation, Regulation, and Litigation

While the prospects of broad general privacy legislation may have diminished in the U.S., other changes are possible. This includes the likely rollback of FCC rules governing privacy practices of broadband and cellular service providers. As to the FTC, House Republicans supported legislation that would impose some limits on FTC actions in adopting regulations or imposing consent agreements in the last Congress,[64] and many of the proposals would be a plus for industry. Preemptive national data breach legislation could greatly simplify the process of responding to potential breaches, but this is not a Republican priority. The prospect of national, preemptive privacy legislation still seems to be an even more remote possibility.

Although not currently on the FTC's agenda, revision to the COPPA Rule is possible during the next Administration. The Rule has been up for revision twice since its initial adoption in 1999. In both 2005 and 2006, the FTC decided to retain it intact. Changes to the Rule adopted in 2012 (and effective in 2013) derived from a 2010 request for information related to technological changes, and an active determination among FTC leadership to change definitions under COPPA to address OBA. Once the FTC has a full complement of Commissioners, discussion of a process to review and update the COPPA Rule with more pragmatic definitions and interpretations is worth exploring. This could include at least a discussion of altering the current strict liability standard for actions by third parties.

Even in an FTC with different priorities, however, we do not see Republicans in Congress or the new Administration abandoning enforcement activity on privacy and security in general and children's privacy in particular. But if enforcement priorities focus on business actions or practices with demonstrable, rather than theoretical, consumer harm, this would be a plus.

Given that many state AGs have higher political aspirations, however, we expect that them to increase enforcement activity over the next four years, possibly working with NGO groups to advance strong privacy protection policies. Litigation

[64] *See* H.R. 5510, *FTC Process and Transparency Reform Act of 2016* (114th Cong., introduced June 16, 2016) (combining multiple reform proposals).

may also play a significantly larger role, underscoring the importance of the legal debate about standing in the courts.

While many things may change, consumer and privacy organizations are expected to continue to highlight privacy and security lapses and use them to expand their anti-advertising agenda. Toy companies and their actions will likely remain in the crosshairs, making continued vigilance to compliance efforts of high importance even if the expectation of new U.S. regulations has decreased. The larger challenge, however, involves dealing with the higher probability of expanding EU restrictions that will affect how toy companies can globally market and advertise their products.

Appendices

Appendix A. OECD Guidelines

Most of today's privacy laws worldwide can trace their origin to the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Data Flows of Personal Data (OECD Guidelines).[65] The OECD Guidelines established eight fundamental principles to protect privacy, with three additional points added in 2013:[66]

- **Collection Limitation:** Data should be obtained via lawful and fair means and generally with the consent of the data subject.
- **Data Quality:** Data should be relevant for the purpose for which it is to be used, and should be accurate, complete and up-to-date.
- **Purpose Specification:** The purposes for which personal data are collected should be specified and subsequent use limited to the fulfillment of those purposes or others compatible with those purposes.
- **Use Limitation:** Personal data should not be used outside the specified purpose except with consent or under authority of law.
- **Security Safeguards:** Personal data should be protected by reasonable security against risks such as unauthorized access, use, destruction, and modification.
- **Openness:** Means should be readily available to establish the nature and existence of personal data, the main purpose of the use, and the identity of the data controller.
- **Individual Participation:** An individual should have the right to obtain information about data collected from them and to have incorrect data erased, rectified, completed, or amended.
- **Accountability:** A data controller should be accountable for effectuating these principles.
- **National Privacy Strategies:** Effective laws should be supplemented by multifaceted national strategies coordinated at the highest levels of governments.
- **Privacy Management Programs:** Organizations should use these as the core operational mechanisms for implementing privacy protections.

---

[65] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. C (80)58 (Final) (Oct. 1, 1980), http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[66] See http://oe.cd/privacy.

- **Data Security Breach Notification:** This provision covers both notice to an authority and notice to an individual affected by a security breach affecting personal data.

The OECD Guidelines encourage the free flow of information where national policies accord with the Guidelines. They also specify that Member countries should generally refrain from restricting transborder data flows of personal information.

Appendix B. U.S. Data Protection Legal Framework

In the U.S., privacy is recognized in a penumbra of constitutional rights, rather than a particular amendment or single overarching law. The U.S. historically relied on a "harms-based" approach to federal privacy legislation, with sectoral laws covering health, financial, and children's privacy, and use of intrusive telecommunications techniques (for example, the Telephone Consumer Protection Act, which restricts telemarketing calls, unsolicited faxes, and automated calls and texts; and the CAN SPAM Act, which restricts commercial e-mail messages).

The FTC enforces privacy and data security violations through its authority over unfair or deceptive acts and practices in Section 5 of the Federal Trade Commission Act.[67] The Electronic Communications Privacy Act (ECPA)[68] and Computer Fraud and Abuse Act (CFAA)[69] also prevent certain intrusions involving computers and digital media. In 1998, concerns about privacy resulted in considerable discussion about general privacy legislation. A narrower law covering children under 13, COPPA,[70] was adopted in 1998. It requires websites and online services directed to children under 13, and those with actual knowledge that they are dealing with a child, to limit collection of personal information from a child and to obtain verifiable parental consent for such collection, with some exceptions.[71]

The FTC continues to enforce violations of the current COPPA Rule. The FTC and the Children's Advertising Review Unit (CARU) have interpreted COPPA to apply to foreign websites directed to children in the U.S.; U.S.-based advertising for a website is one element of the determination that a foreign website is directed to children in the U.S. CARU's guidelines go beyond COPPA by applying a standard under which sites with a "reasonable expectation that a substantial number of children" would visit, "should employ age-screening mechanisms to determine whether verifiable parental consent or notice and opt-out" is necessary, and by seeking to impose age-screening or to limit links to sites not intended for children under 13 that do not engage in neutral age-screening, or both.[72]

---

[67] 15 U.S.C. § 45.

[68] Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*.

[69] Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.

[70] Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq*.

[71] 15 U.S.C. § 6502.

[72] Children's Advertising Review Unit, *Self-Regulatory Program for Children's Advertising* (2009). This was most recently demonstrated by a CARU enforcement action against the well-known Talking Tom app. See http://www.asrcreviews.org/2014/03/caru-reviews-outfit-7s-talking-tom-cat-2-app-recommends-modifications/.

Appendix C. APEC Guidelines

The Asia-Pacific Economic Cooperation (APEC) developed principles for privacy that in some respects modify the OECD principles[73] and are intended as something of a counter to the EU Data Directive, notwithstanding the fact that some countries have adopted legislation that is sometimes modeled on the EU Directive. The APEC Privacy Framework establishes nine high-level privacy principles:

- **Preventing Harm:** Personal information protection should be designed to prevent the misuse of such information.
- **Notice:** Controllers of personal information should provide clear and easily accessible statements about the privacy policy and practices before or at the time the data is collected.
- **Collection Limitation:** Collection should be limited to information that is relevant to the purposes of collection.
- **Uses of Personal Information:** Personal information should be used only to fulfill the specific purposes for which it was collected.
- **Choice:** Users should be provided a clear, prominent, easily understandable, accessible, and affordable mechanism to exercise choice over the collection of their personal information.
- **Integrity of Personal Information:** Personal information should be accurate, complete, and kept current.
- **Security Safeguards:** Personal information should be protected against unauthorized access or unauthorized destruction, use, modification, or disclosure.
- **Access and Correction:** Individuals should have the right to access and correct any personal information held by the data controller.
- **Accountability:** Data controllers should be accountable for complying with measures that implement these principles.

[73] APEC Privacy Framework (Dec. 2005), http://publications.apec.org/publication-detail.php?pub_id=390.