Toy Industry Association White Paper

Privacy and Data Security: Changes and Risks Abound

SECOND EDITION

May 2014

Prepared for the Toy Industry Association by

KELLER AND HECKMAN LLP
1001 G Street N.W. | Washington, D.C. 20001

Approved by
TIA Responsible Marketing to Children Committee

Table of Contents

I. Introduction

A variety of domestic and international laws and regulations, as well as reports, policy initiatives, and self-regulatory standards, govern privacy and data security in a manner that affects toy companies. The situation is further complicated by a bewildering array of differing laws and regulations that apply around the world, and increasing coordination among international policymakers. Allegations of spying by the National Security Agency (NSA) disclosed by Edward Snowden and massive data breaches affecting millions of consumers have only fueled privacy concerns and appear to be contributing to calls for yet more regulation. Despite general agreement on most of the fundamental principles of privacy and data security, laws and regulations differ worldwide because of underlying cultural, social, and legal differences that further complicate the compliance situation for toy companies.

It is clear that privacy concerns are only increasing, affecting the legislative, regulatory, and litigation landscape in ways that will prove challenging to toy companies. In fact, pressure for more laws that protect privacy often is rooted in fear of how companies will use data for marketing purposes. Consequently, advocates seeking more privacy regulation generally are cooperating in support of broader restrictions on advertising. While divisions over policy directions remain, policymakers worldwide are coordinating to advance enhanced requirements to protect consumer and employee privacy, to protect the privacy of children, and to cooperate on important cross-border enforcement initiatives to protect consumers from fraud and identity theft. In this environment, awareness of legal, political, and technological developments is key.

For example, 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 have created uneasiness about "tracking" users online and have caused traditional distinctions between "personal" or "personally identifiable information" (PII) and "non-personally identifiable information" (non-PII) to erode. Technological change and the proliferation of diverse actors in the digital advertising "ecosystem" make it difficult to explain concisely and clearly who collects data, how they use it, and what choices consumers have about how "their" personal data is used. Industries have embraced self-regulatory initiatives in response, but pressure to regulate in this space persists. In fact, the Federal Trade Commission (FTC) and other regulatory bodies take the view that consumers should be able to choose whether to be "tracked," whether or not it involves OBA, and have now taken the view that general privacy legislation is needed in the U.S.

Issues of children's marketing and privacy have become almost inextricably intertwined in an era where digital marketing and content are the norm for even the youngest children. The U.S. adopted the first law protecting children's online privacy in 1998, and has taken a leading role globally in the issue of protecting children online. The Federal Trade Commission (FTC) adopted revised rules implementing the Children's Online Privacy Protection Act (COPPA) in July 2013 that not only impose new restrictions and requirements, but also undercut the traditional distinctions between PII and non-PII that have formed the basis for how companies have managed data for years. Explosive growth in new communications

opportunities offered by mobile devices, coupled with growing interest by children in using these devices, has resulted in expanded interest in mobile privacy, especially, but not exclusively, involving children. Other non-privacy consumer deception and fairness issues linked to mobile app use, including offering paid apps to children or apps that could allow children to purchase products without parental approval, are a growing topic of concern.

New legislative proposals, notably in the EU, now include privacy protections for children and teens ostensibly modeled on U.S. children's privacy law. However, the proposed EU regulation appears to impose a broad obligation to obtain parental consent whenever any data is collected from children. Unless that proposal is significantly revised, there is a substantial possibility that child-directed websites could be shut down, curtailed, or placed behind pay walls to meet the parental consent requirements as drafted.

To formulate a strategy for the Toy Industry Association (TIA), it is important to review the legislative, regulatory, self-regulatory, and litigation landscape, especially since privacy and security lapses are one of the fastest-growing areas of litigation in the U.S.

To put the current situation in context, we start with some background.

II. Background

Current legal discussions about privacy derive from a common framework developed by the Organisation for Economic Cooperation and Development (OECD) more than three decades ago. Despite a general consensus about important elements of privacy, social, cultural, and legal differences have resulted in different legal and regulatory approaches to privacy and data security that can be difficult to reconcile. Briefly, in countries like the U.S., privacy rights are balanced against free speech rights. While there is a constitutional dimension to privacy, privacy is not recognized as an explicit constitutional right akin to the right of free speech so its formal protection is diminished. In the EU and other regions, however, privacy is viewed as a fundamental human right. The "data subject" has what might be described as ownership rights in his or her personal data, broadly defined. That notion of privacy as a more personal fundamental right has strongly influenced recent debates about privacy in the U.S., reflected in the White House's 2012 "Consumer Privacy Bill of Rights." In turn, privacy advocates are urging the White House and Congress to support general privacy legislation embodying this "Consumer Privacy Bill of Rights." At the same time, consistent with an underlying free speech and "right to know" philosophy prevalent in the U.S., our legal environment promotes privacy notices as well as notifications of breaches involving sensitive data. U.S. approaches to notification of data breaches are in turn being embraced in the EU and elsewhere. All of these concepts are being discussed and shared by policymakers.

A. OECD Guidelines

As noted, 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).[1] The OECD Guidelines established eight fundamental principles to protect privacy:

- **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.

[1] 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.

- **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.

These guidelines were updated in 2013 to address the need to use a practical, risk management-focused approach to privacy protection, and to enhance global privacy protection by improving interoperability.[2] The OECD added these to the eight principles noted above:

- **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.
- **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 also encourage the free flow of information where national policies accord with the Guidelines. They also specify that Member countries should refrain from restricting transborder data flows of personal information except where another Member country "does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation."[3] This concept is the origin of the EU's so-called "adequacy" limitation, discussed below, which has created many compliance issues for multinational companies. Adequacy restrictions are appearing in other laws, too, which will again complicate the global compliance landscape for toy companies.

While the U.S. was one of the prime movers of the OECD Guidelines, differences in how the U.S. and EU have chosen to address privacy have been a source of tension and frustration for the business community. In some cases those differences appear to also reflect protectionist tendencies aimed at keeping high-paying technical jobs within the country or region.

[2] See http://oe.cd/privacy.
[3] *Id.*

B. U.S. Data Protection Legal Framework

In the U.S., privacy is recognized in a "penumbra" of constitutional rights. 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 Do Not Fax, Do Not Call, and CAN SPAM laws). The Electronic Communications Privacy Act (ECPA)[4] and Computer Fraud and Abuse Act (CFAA)[5] also prevent certain intrusions involving computers and digital media. In 1998, concerns about privacy resulted in considerable legislative discussion about general privacy legislation. A narrower law covering children under 13, COPPA[6], was adopted with the strong support of many business interests (many lacking a significant presence in the children's space) to avoid broader general privacy legislation. Concerns about online tracking for purposes of serving advertising, however, have resulted in a new chorus seeking a broad, federal general privacy law.

Apart from the federal dimension, privacy is protected under common law. State privacy and security laws may apply, and enforcement of privacy and security violations may occur under federal and state consumer protection laws if practices are deceptive or unfair. Most U.S. states also have enacted data breach notification legislation. Generally, notifications are required where sensitive data – including Social Security numbers, driver's license information, or bank account information – is disclosed. In California, recent changes deem e-mail addresses to be personally identifiable information when used with passwords to constitute log-in credentials, thus making the inadvertent disclosure of those email addresses a notifiable breach under that state's laws.

Children's data or data from teens is not considered sensitive personal data per se under any state data breach law. However, pressure to enact broader restrictions on the ability to collect information from minors continues. Organizations such as the Campaign for a Commercial-Free Childhood (CCFC) and the Center for Digital Democracy (CDD) have supported strong privacy legislation as part of their agenda to restrict advertising to children and teens. California recently adopted a law that will require Internet websites and mobile app operators to offer an "eraser button" to minors to remove content posted on the relevant site or app. Further, interrelated discussions of advertising and privacy refer to research on the cognitive ability of kids and teens to understand and defend against advertising, and to more recent research suggesting that teenagers' brains are not fully developed. Advocates suggest that this makes all minors more vulnerable to impulsive behavior that can be problematic in the online sphere, and urge further restrictions on both advertising to and collecting data from teens and children alike.

Historically, while the U.S. lacks a general privacy law, some provisions of U.S. law are significantly more restrictive and proscriptive than other data protection laws outside the U.S. One other notable feature of the U.S. landscape is the significantly greater amount of private litigation compared to other regions. There has been a sharp increase in privacy and data security lawsuits over the past few years, a trend that shows no sign of abating. Asserted privacy violations reflected in press articles, announcements of data breaches, and alleged failures to adhere to stated privacy and security policies have been the basis

[4] Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq*.
[5] Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.
[6] Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq*.

of multiple lawsuits, including class action lawsuits, around the country, as well as regulatory enforcement action.

C. EU Data Protection Legal Framework

The EU deems privacy a fundamental human right. While privacy rights are not absolute and are subject to the concept of "proportionality," consumers (and employees) in the EU have more extensive legally recognized privacy rights than in the U.S. Special limits apply to sensitive data, such as race, ethnicity, and trade-union membership, so it is defined differently than in the U.S. under state data breach or federal sectoral privacy laws. Importantly, the EU Directive on Data Protection restricts transfers of data from the EU to countries lacking an "adequate" system of privacy.[7] There are several ways to accommodate data transfers to meet the "adequacy" standard. Each adequacy mechanism has its own limitations and problems, however.

The U.S. Department of Commerce (DOC) and European Commission agreed to a negotiated "safe harbor" to accommodate transfers to the U.S. at the time that the Data Protection Directive went into effect. This effectively is a self-certification of compliance with the requirements of the Directive, and requires an annual filing with DOC. The safe harbor has had a number of vocal critics among privacy advocates and national EU data privacy regulators. The FTC recently announced more than a dozen settlements with companies that it alleged falsely claimed current registrations with the DOC under the safe harbor framework.[8] These publicly touted enforcement initiatives suggest recognition by the U.S. government of increasing concern about the effectiveness of the safe harbor in some EU circles, and should be viewed as a strong indication of U.S. government support for the safe harbor, which continues to be backed by many in the business community.

Other instruments to assure adequacy available under EU law include inter-company agreements and binding corporate rules (BCRs). Inter-company agreements can work well when companies are structured through a few regional holding companies, but can create dizzying complexities for large multi-national businesses with many subsidiaries and affiliates. BCRs were intended to provide a vehicle for companies to clarify their privacy policies without the contractual complexities. In practice, however, data protection administrators often still require that companies enter into intra-company contracts binding corporate affiliates to uphold the BCRs, and requirements that companies agree to take steps beyond those required by law have created significant concerns. Additionally, the BCR approval process can be extremely cumbersome.

While dealing with transfers just within a family of companies is challenging enough, data processing by third parties must generally be covered by processor agreements, introducing other logistical and legal complications.

[7] Directive 95/46/EC.
[8] *See* FTC, *FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework* (Jan. 21, 2014), http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply.

Violations of privacy laws can result in criminal penalties as well as civil penalties or private actions, but to date enforcement has not been consistent or always robust in the EU. There is a distinct sense that major U.S. businesses are the favorite target for government enforcement agencies. However, private lawsuits are rare in the EU largely because class action options and contingency fee opportunities are limited, permitted discovery is not typically as extensive as in the U.S., and "loser pays" rules may apply. Further, differences in enforcement philosophy have generally meant that liability exposure for privacy or security lapses is higher in the U.S. than in the EU despite more restrictive, general privacy laws in the EU.

The EU privacy legal framework takes on added importance as other jurisdictions have adopted similar laws modeled on the EU Directive in an effort to attain "adequacy." For example, the EU approach has influenced laws and proposals in South America and Asia, but some jurisdictions, like Canada and Australia, have adopted laws that are more of a hybrid of the U.S. and EU approaches. Recent changes to the Australian privacy law, however, reflect a more proscriptive approach more in keeping with the EU system. Despite the efforts of non-EU countries to adopt laws that protect privacy, the EU recognizes very few jurisdictions as having adequate privacy regimes.

In 2012, the EU proposed an extensive overhaul of its privacy legal framework that would impose extensive new restrictions. One key change is the move to alter the current Directive framework, which has to be enacted through implementing national legislation, and instead adopt a regulation, which would apply as law throughout EU Member States. The proposed regulation includes new restrictions on information collection from children that could virtually shut down or require restructuring of many child-directed websites. In addition, the proposed regulation purports to have extraterritorial effect, applying to the collection of information about EU citizens anywhere in the world. It also creates a penalty structure that could impose penalties of up to 2% of global annual turnover.[9] A plenary vote in the European Parliament resulted in some changes to the draft regulation, including an increase in penalties to €100,000,000 or up to 5% of global annual turnover. The regulation must be adopted through a co-decision process involving the European Council of Ministers, and additional changes in the regulation are possible despite press statements from the EU's Justice Minister that the regulation is now "set in stone."[10]

D. APEC Guidelines

The Asia-Pacific Economic Cooperation (APEC) developed principles for privacy that in some respects modify the OECD principles[11] and are intended as something of a counter to the EU Data Directive,

[9] See proposed Regulation, Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); proposed Directive, Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Background information is available at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

[10] *See* European Commission, Memo, *Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote* (Mar. 12, 2014), http://europa.eu/rapid/press-release_MEMO-14-186_en.htm.

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

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.

In late 2011, APEC leaders approved Cross-Border Privacy Rules (CBPRs) that create a role for self-regulation, but with added oversight through third party certification (see more below). The hope is that strong self-regulation will halt expansion of EU-style privacy laws and create a scheme of "light touch" regulation that relies on self-regulatory organizations to be the first stop for complaints. APEC and the EU also recently announced plans to map APEC's CBPRs and the EU's BCRs onto each other, which in theory would simplify the process for entities seeking "double certification" under the two regimes.[12] Whether that type of harmonization will be achieved in practice remains to be seen.

[12] The Joint work between experts from the Article 29 Committee and from APEC economies was announced on March 14, 2014, http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

III. Significant U.S. Laws and Policy Developments

As noted above, the U.S. legal landscape has been dominated by a fragmented system of privacy and data security laws that rely largely on a harms-based approach to the regulation of privacy and data security. Legislation tends to be sector- and medium-specific, unlike the general framework approach in the EU and elsewhere. Another feature that differentiates the U.S. legal landscape from other regions' is the ready availability of private litigation, most notably class action litigation. State legislation dominates in some areas, like data breach notification requirements, while federal legislation applies in others (to the exclusion of state laws). The U.S. was the first jurisdiction to adopt national children's privacy legislation, and toy companies that operate websites and online services geared to children are no doubt very familiar with this law.

A. FTC Amends COPPA Rule

The U.S. adopted COPPA 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.[13] FTC proposed dramatic changes to the implementing regulations in 2011,[14] which drew substantial comments from many stakeholders, including TIA. FTC released a final rule in January 2013, which went into effect on July 1, 2013.[15] The changes, while much less onerous than originally proposed because they incorporated revisions that addressed concerns raised by TIA in its written comments, still pose significant challenges to toy companies. Important changes include the following:

- **Personal Information:** The term "personal information" now includes "persistent identifiers" linked to a device like Internet Protocol (IP) addresses or Uniform Device Identifiers (UDIDs) (except when used to support the internal operations of a website or online service, discussed in more detail below); geolocation information; and photos or audio files of children.
- **Operator:** Operators of child-directed sites and services will be strictly liable for all information collection that occurs at their website or online service, including by third parties.
- **Website or Online Service Directed to Children:** The FTC will continue to apply a multi-factor test to determine if a site or online service is directed to children. If a site is only secondarily directed to children, the operator can implement an age-screen before collecting the broader types of information that can be collected from teens or adults. Likewise, any site or online service that has actual knowledge that it is collecting personal information can be liable under COPPA. A website is not deemed to be directed to children merely because it links or refers to a website that is directed to children.
- **Support for Internal Operations:** Collection and use of persistent identifiers at a child-directed website is permitted for purposes such as to maintain or analyze the functioning of the website;

[13] 15 U.S.C. § 6502.
[14] Children's Online Privacy Protection Rule, proposed rule, 76 Fed. Reg. 59,804 (Sept. 27, 2011).
[15] *Children's Online Privacy Protection Rule, final rule*, 78 Fed. Reg. 3,972 (Jan. 17, 2013), http://www.ftc.gov/sites/default/files/documents/rules/children's-online-privacy-protection-rule-coppa/130117coppa.pdf.

perform network communications; authenticate users of or personalize content on the website; serve contextual advertising; protect the security or integrity of the user, website or online service; ensure legal or regulatory compliance; or fulfill the request of a child as otherwise permitted in the rule. The FTC also indicated that intellectual property protection, payment and delivery functions, spam protection, optimization, statistical reporting, and de-bugging functions are also covered. Information that may be used or disclosed to contact a specific individual, develop a profile on a specific individual, engage in OBA, or for other purposes is not included in the definition of permitted "support for the internal operations." Operators may submit requests for approval of additional activities that may be included within the definition of "support for internal operations."

- **Verifiable Parental Consent:** Despite initially proposing to remove it, the final rule retained "e-mail plus" as an acceptable parental consent method for operators collecting personal information only for internal use. This method of parental consent has been critically important for toy companies offering online sweepstakes and contests, and retaining this as an option for parental consent was critically important to the industry. Other acceptable methods of parental consent that may be used when e-mail plus options do not apply include electronic scans of signed consent forms; video-conferencing or manned toll-free numbers; government-issued identification, such as a driver's license or partial Social Security number; and credit card, debit card, or other online payment. The FTC has approved parental consent methods offered by various intermediaries who require full or partial SSNs, but these methods do not appear to be favored by consumers or by toy companies.

- **Notice:** Notice of privacy practices must appear in a posted privacy policy. Direct notice of the operator's practices to parents is mandatory in certain circumstances as well. Direct notice requirements are intended to ensure that key information is provided to parents, with succinct "just-in-time" notice being favored. This includes information already collected from the child, the purpose of the notice, the action that the parent must or may take, and what use (if any) the operator will make of the personal information collected.

- **Confidentiality, Security, and Data Retention:** The final rule includes enhanced requirements for operators to maintain confidentiality and secure children's personal information, with a new provision addressing data retention and deletion. Operators must take reasonable steps to release children's personal information only to service providers or third parties who are capable of maintaining its confidentiality, security, and integrity, and provide assurances to that effect. Children's personal information may be retained only so long as reasonably necessary to fulfill the purpose for which the information was collected.

- **Safe Harbor:** Safe harbor programs must ensure that participating operators provide substantially the same or greater protections for children as required in the rule. An effective mandatory program for the independent assessment of compliance includes the conduct of annual, comprehensive reviews of each of their members' information practices, and disciplinary action for non-compliance (including actions like mandatory public reporting, consumer redress, voluntary payments to the U.S. Treasury, and the referral to the FTC of operators who engage in a pattern or practice of violation). Organizations seeking safe harbor status must meet detailed requirements for approval. Approved safe harbor organizations must submit aggregated summaries of independent audits and disciplinary actions against member operators to the FTC annually, and respond promptly

to FTC staff inquiries. This expressly includes making available to the FTC copies of consumer complaints, records of disciplinary actions taken against operators, and results of the independent assessments of participants.

Several changes to the final rule from the proposed rule responded to TIA's concerns, including rejecting the notion that passwords and login names would be considered personal information, retaining e-mail plus as a mode of parental consent, broadening the definition of actions that constitute support for the internal operations, and making the monitoring of safe harbor programs, while still onerous, less intrusive than originally proposed.

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 also go beyond COPPA in applying a standard under which sites with a "reasonable expectation that a substantial number of children" would visit the site, and seeks 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.[16]

CARU is also one of six organizations that have received FTC approval for their safe harbor programs since the initial rule took effect in 2000. The FTC continues to receive, consider,[17] and approve applications for participation. Other groups include TRUSTe and the Entertainment Software Rating Board (ESRB). In settlements over violations of the COPPA Rule, the FTC has required settling firms to either retain an online privacy professional or join an approved safe harbor program.[18]

B. Government / Private Sector Data Breaches Roil Worlds of Cybersecurity and Privacy

Following the 2010 release of diplomatic cables by Chelsea Manning (then Bradley Manning), a new river of documents about covert U.S., British, Australian, and other foreign classified surveillance programs began flooding the media in June 2013. NSA contract employee Edward Snowden and lawyer-journalist Glenn Greenwald have revealed government surveillance that allegedly includes metadata and content from mobile phone calls, e-mails, and other activities tied to citizens in the U.S. and around the world. While observers disagree as to whether Manning, Snowden, and the reporters who help them are traitors or whistleblowers shining the light on illegal government actions, the revelations have prompted high-level contacts between the U.S. government and its counterparts – particularly in Europe – and exacting congressional and public scrutiny. The revelations also contributed to the deep suspicion about the different approaches to privacy in the U.S. by European and other regulators. In turn, this has greatly complicated the ability of U.S. businesses to engage with policymakers about the upcoming EU Privacy Regulation.[19]

---

[16] 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 www.asrcreviews.org/2014/03/caru-reviews-outfit-7s-talking-tom-cat-2-app-recommends-modifications/.

[17] See, e.g., FTC, FTC Seeks Public Comment on iKeepSafe's Proposed Safe Harbor Program Under the Children's Online Privacy Protection Rule (Mar. 13, 2014), www.ftc.gov/news-events/press-releases/2014/03/ftc-seeks-public-comment-ikeepsafes-proposed-safe-harbor-program.

[18] See, e.g., FTC, Operator of Social Networking Website for Kids Settles FTC Charges Site Collected Kids Personal Information Without Parental Consent (Nov. 8, 2011), www.ftc.gov/news-events/press-releases/2011/11/operator-social-networking-website-kids-settles-ftc-charges-site.

[19] *See* http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

The private sector was rocked in December 2013 by reports that the large U.S. retailer Target had its payment systems infiltrated by hackers during the holiday season, compromising the information of between 40 and 70 million in-store shoppers. Breaches from other prominent retailers soon followed. While over the years millions and millions of consumer records have been breached, the Target incident seemed to create a tipping point in the debate about data security. Payment-system operators, banks, and retailers have since alternately accused each other of being responsible for lax security and promised to work together to shore up the U.S. payment system. Indications are that the U.S. will shift from magnetic stripe technology to chip and PIN technology for credit cards within the next two years.

Both of these events have dramatically shifted the public's attention to matters of privacy and cybersecurity, and appear to have made the public expect reports of breaches of their information earlier, based on less concrete information, and with greater contrition on the part of affected companies. Litigation has already started and legislation related to each of these issues has been and likely will continue to be proposed. Now more than at any time since the adoption of COPPA it appears that broad new privacy laws may pass in Congress. Actions in the private sector, such as the implementation of new payment systems in the U.S., should be expected.

C. White House Promotes Release of New Cybersecurity Framework

In the wake of the major public and private data breaches discussed immediately above, President Obama recently announced the release of the final version of a Cybersecurity Framework[20] (a follow-up to his announcement of a plan to develop such a framework one year earlier).[21] The Framework was developed by the National Institute of Standards and Technology (NIST) in concert with a broad array of private and public sector stakeholders to help identify and communicate about cybersecurity risks. It is broad and relatively non-specific because its framers meant for diverse entities to use it. The five core concurrent and continuous functions specified are identifying risks and key information assets, protecting the key information identified, detecting breaches, responding to those breaches, and recovering from those breaches. Although the Framework is voluntary and meant to apply to critical infrastructure components, it has a more-than-fair chance of becoming a standard of care in contracts. There is also the potential for the Framework to be cited in private litigation by regulators, insurers, and private parties, even in cases of data breaches far outside of the critical infrastructure core. Given the voluntary nature of and the broad language contained in the Framework, however, the applicability of specific cybersecurity measures will likely depend on companies' size, sophistication, and use of technology.

D. Legislation

- **Do Not Track Kids Act.** Versions of this act have been proposed in 2011 and 2013, and would ban the tracking of kids and expand privacy protections for teens.[22] Initially proposed only in the House

[20] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), http://www.nist.gov/cyberframework/.
[21] Exec. Order 13,636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11,739 (Feb. 19, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[22] 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.

by then-Rep. Markey (D–MA) and Rep. Barton (R–TX), the bill has gained senatorial sponsors by Markey's elevation to the Senate and his being joined by Sen. Kirk (R–IL). FTC pronouncements indicate support for the concept of an "eraser button" to protect privacy.

- **General Privacy, Mobile Privacy, Do Not Track Legislation, Data Breach Legislation.** Many other privacy bills have been introduced to limit tracking in general and establish "baseline" privacy protections. In the past few months, no fewer than three Senate committee chairs have proposed privacy, data security, and cybersecurity legislation. While too numerous to review in detail in this white paper, the many Congressional bills touching on privacy reflect strong interest in federal legislation and the growing importance of privacy and data security as a core public policy issue. As noted previously, it appears more likely now than at any time in almost two decades that Congress will adopt general privacy legislation.

E. Guidance and Self-Regulation

- **White House, FTC Privacy Reports.** In 2012, the Administration released two reports proposing an expanded scope of privacy in the form of a "Consumer Privacy Bill of Rights."[23] While supportive of some self-regulatory efforts – in particular the Digital Advertising Alliance (DAA) programs for OBA – the reports say that industry self-regulatory efforts on mobile apps do not go far enough. Both reports support adoption of "multi-stakeholder enforceable codes of conduct." The concept raises serious potential legal concerns because treating such codes as enforceable without conducting a rulemaking bypasses established administrative procedural protections governing rulemakings. A coalition of privacy and cybersecurity groups led by the Electronic Privacy Information Center (EPIC) urged the administration to push Congress to adopt the administration's proposal privacy bill of rights as law in early 2014.[24]

- **FTC Dings Mobile Apps, Outside Groups File Complaints Against Companies.** In 2012, the FTC released a report suggesting that privacy policies are inadequate or lacking in kid-directed apps and urged short, effective disclosures.[25] Since then, the agency has received multiple complaints from consumer groups alleging COPPA violations by websites and apps, including against prominent brand owners. The FTC investigates all allegations of possible violations of COPPA by third parties, and also periodically "surfs" the digital landscape to identify potential issues. With privacy protection a key priority for the FTC, it will bring enforcement actions if it believes it has grounds to do so.

- **NTIA Developing Multi-Stakeholder Codes of Conduct.** In the wake of the 2012 White House report, the National Telecommunications and Information Administration (NTIA, an arm of DOC) held a meeting on developing privacy codes of conduct.[26] NTIA identified mobile apps as the first topic for multi-stakeholder action. A proposed code of conduct was released in July 2013, which

[23] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (February 2012); FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (March 2012).
[24] Letter from EPIC, et al., to Pres. Obama (Feb. 24, 2014), http://epic.org/privacy/Obama-CPBR.pdf.
[25] FTC, *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing* (Feb. 2012), http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.
[26] *Multistakeholder Process To Develop Consumer Data Privacy Codes of Conduct*, 77 Fed. Reg. 13,098 (Mar. 5, 2012); comments are available at http://www.ntia.doc.gov/federal-register-notice/2012/comments-multistakeholder-process.

would require app developers, if they choose to subscribe to it, to use a short-form notice to explain what data they collect, let users access a long-form policy, and disclose the sharing of user-specific data and the identity app operator. Both user-created and automatically-collected data are covered by the code.[27] NTIA pronounced itself pleased with the effort and industry groups did participate in the multi-stakeholder process, but NGOs have criticized it with the CDD, calling for the FTC to replace NTIA in the process. One relatively new organization, the Application Developers Alliance (ADA), released open-source code to enable app developers to comply with the Code of Conduct.[28] However, despite its statement of support for the NTIA Code, the FTC has not officially indicated that compliance will satisfy the requirements of COPPA, and there is little incentive for companies to publicly proclaim that they will comply with the NTIA guidelines as infractions will subject them to FTC enforcement action for deceptive statements about compliance. NTIA is proceeding with the development of a second multi-stakeholder code of conduct, this one on facial recognition technology.

- **FTC Releases Updated DotCom Disclosures.** In March 2013, the FTC's staff released an update to the DotCom Disclosures guidance first published in 2000.[29] The purpose of the update was to highlight issues in the mobile space and other online technologies. In general, disclosures required to prevent an advertisement from being unfair, deceptive, or misleading must be presented "clearly and conspicuously." Given the limitations of mobile devices (particularly with regard to screen size), the FTC pointed out that disclosures are more likely to be effective if consumers view disclosures and claims close to one another. Other pieces of guidance include providing disclosures before purchases and limiting distracting factors. The only mention of children in this edition was to mention in a footnote that representations to specific groups, like children, will be judged by how a reasonable member of that group would be affected by the practice.

- **Privacy Self-Regulation.** Many self-regulatory initiatives have sprung up to advance privacy. COPPA includes a "safe harbor" component that allows companies to participate in recognized safe harbor programs approved by the FTC, but general privacy and children's privacy safe harbor programs exist. For example, CARU, the Council of Better Business Bureaus (CBBB), the ESRB, TRUSTe, and others offer safe harbor privacy programs.[30] The revisions to the COPPA Rule adopted more extensive oversight of children's privacy safe harbor programs and program participants, and such programs must be approved by the FTC. Some general proposed privacy legislation expands on the safe harbor concept. The notion of multi-stakeholder enforceable codes of conduct appears to take the concept one step further into the murky legal realm of co-regulation. The DAA's self-regulatory program for online behavioral advertising garnered positive expressions of support in an FTC report; enforcement efforts are underway and technical discussions about expansion to mobile media continue. The Network Advertising Initiative (NAI), in existence since 2000, adopts, updates and enforces a code of conduct applicable to third party network advertisers. While the Mobile Marketing Association (MMA), DAA, NAI, and CTIA have issued self-regulatory guidance on mobile

[27] NTIA, *Privacy Code of Conduct* (draft July 25, 2013), http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.
[28] ADA, *Open Source Code for Mobile App Privacy Notices* (Mar. 2014), http://devsbuild.it/privacynotices.
[29] FTC, *DotCom Disclosures* (Mar. 2013), http://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-staff-revises-online-advertising-disclosure-guidelines/130312dotcomdisclosures.pdf.
[30] CARU actually monitors online privacy activities of kid-directed websites whether or not companies are formal participants in the CARU Safe Harbor program, and the CARU Guidelines go beyond COPPA, covering websites where there is a reasonable expectation that a significant number of children will visit.

apps, mobile app privacy initiatives have been characterized as "needing improvement," and much of the control lies in the hands of app developers and app platform providers. As noted above, apart from privacy and data security considerations, other questions include whether ads are identifiable as such and whether in-app purchase procedures are appropriate.

F. Enforcement and Litigation

- **FTC, California Attorney General Argue that COPPA Does Not Preempt State Privacy Laws.** In one prominent class action lawsuit against Facebook, both the FTC and the California Attorney General weighed in to argue that COPPA does not preempt state requirements to obtain parental consent for use of a teenager's name or likeness in advertising. The filings came in connection with a proposed challenge to a settlement of a lawsuit filed against Facebook for using names and likenesses of individuals who "friend" brands in sponsored advertising.[31] A settlement was reached, but is being challenged by CDD in the Ninth Circuit,[32] the venue where the FTC and California AG briefs were filed. A ruling that narrowly defines the scope of preemption is much more likely given the FTC and California AG's position that COPPA does not preempt state law. Such a ruling would be a potential game-changer: if the courts side with the FTC and California, it will also likely prompt further state legislative action designed to protect teen privacy that will no doubt affect advertising practices as well. Thus, the court's ultimate decision here could have profound implications on all websites, and is one that should be closely watched.

- **AGs Set Sights on Children's Privacy.** New Jersey's Attorney General recently settled its second claimed violations of COPPA and state law. The targets of the parens patriae actions were app developers in both cases, and both developers were based in California.[33] The ramifications of these actions thus reach website and online operators across the country. California's Attorney General has also been active in this area, previously obtaining agreements with several major app platform developers to provide privacy policies in accordance with COPPA. Maryland created an Internet Task Force, the brainchild of the state's Attorney General, currently a candidate for governor. Protecting privacy is politically popular, and independent actions by state attorneys general are increasingly likely in this landscape.

- **Privacy and Data Breach Litigation.** Private lawsuits related to alleged privacy or data security lapses are on the rise, including class action lawsuits. Suits are common in the wake of data breaches; the most prominent recent breach – Target's – has triggered several dozen suits, including some by financial institutions. In other cases, lawsuits have been filed based on alleged failure to adhere to privacy commitments in posted privacy policies, for the use of technology that changes browser settings or preferences, and for technology that accesses information like contact lists or geolocation information without permission. Changes in privacy policies have triggered litigation,

[31] See, e.g., E.K.D., et al. v. Facebook, Inc., 12-cv-01216 (N.D. Cal., Mar. 8, 2012).
[32] CDD, Public Citizen, Children's Advocacy Institute & CDD Oppose Facebook Sponsored Stories Deal That Threatens Teen Privacy/CCFC Rejects Facebook Settlement, Turns down $290K (Feb. 13, 2014), http://www.democraticmedia.org/public-citizen-childrens-advocacy-institute-cdd-oppose-facebook-sponsored-stories-deal-threatens-tee.
[33] See Office of N.J. Atty. Gen'l, Acting Attorney General Announces Settlement Resolving Allegations That Maker of "Dokobots" App Violated Children's Online Privacy Rules (Nov. 22, 2013), http://nj.gov/oag/newsreleases13/pr20131122a.html; Office of N.J. Atty. Gen'l, App Developer, Sued By New Jersey Attorney General and Division of Consumer Affairs, Agrees to Stop Transmitting Personal Information on Children, And Will Ensure Transmitted Information is Destroyed (June 27, 2012), http://www.nj.gov/oag/newsreleases12/pr20120627a.html.

as occurred with a recent privacy policy update by Google (which also generated enforcement action in several EU Member States).

- **App Litigation: Payment Issues.** More recently, Apple settled charges that its App Store permitted minors to incur excessive charges on their parents' payment cards through in-app purchases (and later settled the same charges with the FTC),[34] and Google faces similar allegations in a class action suit.[35] While similar questions apply to the issue of whether minors have the capacity to agree to privacy policies and website terms, as a practical matter the growth in paid apps that allow children to incur hundreds or even thousands of dollars in charges raises concerns similar to those previously raised by 900 numbers and texting.

[34] FTC, Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent (Jan. 15, 2014), http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million.

[35] *Imber-Gluck v. Google*, Case No. 5:14 CV-01070-PSG (N.D. Cal., Mar. 7, 2014), https://s3.amazonaws.com/s3.documentcloud.org/documents/1070126/class-action-against-google-over-in-app-purchases.pdf.

IV. Significant International Laws and Policy Developments

Use of digital media can implicate global privacy and telecommunications laws and regulations. While a complete review is beyond the scope of this white paper, a short summary of some key international laws, policy instruments, and self-regulatory activities appears below.

A. EU Privacy Directive and "Cookie" Directive; Proposed Privacy Regulation

Two important directives and their implementing national legislation establish privacy rights in the EU and impose an obligation to disclose use of cookies and get consent. The EU Privacy Directive (Directive 95/46) was adopted in 1995 and entered into force in 1998. Consent is generally required to process personal data, which is broadly defined. Transfers to countries lacking an adequate scheme for privacy are prohibited unless approved legal mechanisms are used. However, in some cases (e.g., employee data) consent is not permitted for some processing or for transfers to countries lacking adequate protection of privacy on the theory that consent cannot be "freely given" where the bargaining power between the parties is unequal. The Electronic Communications Privacy Directive (Directive 2002/58, amended by Directive 2009/136) covers the use of cookies. Consent will be required to use cookies (with some exceptions). OBA remains a controversial issue in the EU. A key body that issues opinions on privacy, the Article 29 Working Group, issued an opinion in December 2011 saying that the industry's self-regulatory program on OBA does not meet the requirements of the e-Privacy Directive, in part because of the opt-out approach for most types of OBA.[36]

As noted above, a proposed EU Regulation would replace the Privacy Directive, establishing for the first time special protections for minors (that is, all persons under 18) and a requirement that sites obtain verifiable parental consent before collecting information from children under 13. The Regulation purports to apply to any entity collecting information from or about EU citizens wherever that business is located, effectively seeking to impose EU law even where websites or services are not intentionally targeting EU citizens. In addition, as indicated above, the new proposed penalty approved by the Parliament of 5% of annual turnover – an increase from the original proposed 2% number – raises the stakes to an even more dramatic degree for violations, particularly since many major U.S. businesses feel that they are likely to be singled out for enforcement.

Many aspects of the proposed Regulation raise serious concerns, and it is so complex that it is difficult to draw attention to the children's provisions, which are of vital interest to many toy companies. This is exacerbated by the small number of companies interested in the children's privacy provisions in comparison to the larger number of businesses affected by other more general obligations in the proposed Regulation. However, because the EU defines "personal information" quite broadly – and generally includes persistent identifiers – the result of the proposal would be potentially devastating to many toy companies because the proposal does not specifically recognize any of the exceptions that help make COPPA, burdensome as it is, more workable.

[36] Article 29 Working Party, Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising (December 8, 2011).

For example, there is no indication that persistent identifiers could be collected for analytical or other uses that help support the website's operation, no mechanism to allow a company to collect a child's e-mail address to respond to a one-time question, and no suggestion that less robust methods of parental consent, like e-mail plus, would be acceptable where the data would solely be used for internal marketing purposes. This combination – and the absence of other relevant exclusions or clarifications – may well result in elimination or curtailment of free online content for children. Instead, the Regulation delegates authority to the European Commission to establish rules. Additionally, the potential scope of the proposal, including the statement that the Regulation will apply whenever and wherever personal information from EU citizens is collected will create potential challenges, perhaps resulting in the need for a geographic screen at websites to exclude the possibility that personal information from EU residents will be collected, or to post a specific opt-in to such collection.

To enter into force, the Regulation must be approved by the EU Council and Parliament through a co-decision procedure. Political discussions on the subject continue, and a final decision was recently put off until the end of this year or early next year.

B. Other EU Member State Developments

- **International Privacy Cooperation and Coordination.** The Information Commissioner's Office (ICO) of the United Kingdom signed a memorandum of understanding (MOU) with the FTC to bolster joint privacy enforcement. (The ICO is the UK's privacy enforcement agency.) Separately, as noted previously, the FTC announced that officials from the EU and APEC agreed to work on mapping APEC's CBPRs and the EU's BCRs onto each other.[37] When completed, the project's output is meant to serve as a practical reference tool for companies that wish to obtain "double certification" under both systems. Separately, the UK's Office of Fair Trading released a set of principles for online and app-based games shortly before it was replaced by the Competition and Markets Authority (CMA). The principles are intended to address concerns revealed after an April 2013 investigation in which the authority found insufficiently transparent, accurate, or up-front cost diclosures and "exploitation" of children's relative inexperience.[38]

- **Three EU Members Fine Google.** Authorities in France, the Netherlands, and Spain have each declared that Google Inc. violated national laws when it modified and updated its privacy policy in 2012. Notably, each country leveled its charges against the U.S. entity, not the Google entity operating in its own country. This move contributes to the fear that there are protectionist motivations behind European governments' privacy enforcement efforts. French officials imposed the highest fine available under its legislation: €150,000 ($203,000). Google is appealing the fine. Earlier, Spain assessed a €900,000 ($1.2 million) fine, and the Netherlands declared the privacy policy changes a violation of Dutch law, waiting until after a hearing to decide on any enforcement measures. Three other countries are reported to be investigating bringing similar charges: the United Kingdom, Germany, and Italy. The muscle-flexing in terms of privacy enforcement

[37] See Article 29 Work Party & APEC Economies, Referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents (Mar. 6, 2014), http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.
[38] *See* OFT, *Principles for online and app-based games* (Jan. 2014), http://www.oft.gov.uk/shared_oft/consumer-enforcement/oft1519.pdf.

suggests the potentially enormous adverse implications of the penalty structure under the proposed EU Privacy Regulation, as well as the likelihood that U.S. companies whose primary activities involve data collection targeting consumers in the U.S. could nevertheless be charged with violating EU law.

- **Germany.** After the Snowden-NSA revelations, Chancellor Angela Merkel announced support for proposals that would create data networks to keep e-mails and other communications inside Europe and out of the reach of U.S. intelligence agencies. She herself was reported to have been a target of spying operations, as were other world leaders. The notion of "data localization" appears to be spreading.

C. APEC and Latin America

- **Canada.** Canada has a series of provincial and federal privacy laws that incorporate elements of U.S. and EU policy approaches, combining some general privacy and data protection laws with sector specific requirements. The Office of the Privacy Commissioner investigates complaints related to the federal Personal Information Protection and Electronic Documents Protection Act (PIPEDA). PIPEDA does not include special provisions on children's privacy. Private sector complaints in provinces with substantially similar laws to PIPEDA (Alberta, British Columbia and Quebec) are handled at the provincial level. Efforts are made to negotiate a resolution, but the Privacy Commissioner does have subpoena and related enforcement powers. The Privacy Commissioner's case findings are available online.[39]

- Sector-specific laws also apply. The Canadian Radio-Television and Telecommunications Commission (CRTC) recently released final regulations implementing Canada's anti-spam law, for example.[40] The Canada Anti-Spam Law will come into effect in July 2014, and applies whenever a computer in Canada sends a commercial electronic messages anywhere in the world, regardless of whether the destination is in Canada.[41] In this regard, Canada does appear to apply a "country of origin" test in seeking to assert jurisdiction over the communication.

- Regulatory bodies in Canada also provide guidance, much as is done in the U.S. The Privacy Commissioner published guidelines for online behavioral advertising that are encouragingly in line with the U.S. self-regulatory initiative. Provincial privacy leader Ann Cavoukian has promoted the concept of "privacy by design," which is being embraced globally.

- **South America.** Argentina was one of the first countries in South America to adopt an EU-style general privacy law; it is modeled on Spain's law and incorporates a habeas data right recognized in the constitution. Mexico adopted a general privacy law in 2010; implementing regulations were finalized in December 2011. The Mexican law distinguishes between personal data (broadly defined) and sensitive data, and recognizes rights of access, rectification, cancelation, and opposition (often called "ARCO rights"). Mexico does not include an adequacy limitation like that in the EU Directive, and does not impose special provisions on children's privacy. Colombia, however, passed a data protection law in October 2012 that, like the law in Argentina, generally follows the

[39] Findings available at http://www.priv.gc.ca/cf-dc/2009/index2-9_e.asp.
[40] Canadian Radio-television and Telecommunications Commission (CRTC), *Electronic Commerce Protection Regulations* (Mar. 2012).
[41] *See* http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00211.html.

EU approach. Brazil passed a bill in March 2014 that created an Internet Bill of Rights, which would permit Brazilian officials to access information extraterritorially if it touches on matters they deem relevant to their interests or investigations. (Previous versions of the bill would have required ISPs to keep all relevant data on servers in Brazil.) The bill also requires companies to obtain express consent from Brazilian users before processing personal data online, and may make the unauthorized transfer of data outside the country illegal, even for processing and storage.

- **Asia and Oceania.** Privacy laws have been in place for years in Australia (see below), New Zealand, and Hong Kong, and legislation has been proposed or adopted in many significant countries, such as India and China. China has a spam law that includes elements of the EU and U.S. requirements; it is still discussing a general privacy law. India issued Privacy Rules recently that included policy elements from the EU Directive. Singapore passed a law in 2012 that establishes a baseline data protection framework and a do-not-call registry, among other features. It goes into effect in July 2014.

- **APEC Framework.** As indicated above, the APEC privacy principles are intended to counter the spread of EU Directive-like legislation in the APEC region, and to create a system endorsed by regional governments that allow for a type of self-regulatory approach to be recognized. The APEC Framework includes CBPRs intended to govern the internal process by which businesses address privacy. They were approved at the leaders meeting in November 2011. The CBPRs involve third party review and certification of corporate privacy policies and practices. Compliance with the APEC Framework is expected to be a minimum standard; compliance with domestic laws will also be required. However, the hope is that the APEC framework will promote harmonization of laws and requirements throughout the region and offer a mechanism to accept a type of "binding corporate rules" for data transfers.

- **Australia Amends Privacy Law.** More recent developments may have undermined that hope. Although the Australian government has been closely involved in the development of the APEC Guidelines, Parliament approved the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 Act in November 2012.[42] The Act establishes a single, national set of Australian Privacy Principles (APPs) applying to both commonwealth agencies and private sector organizations. The use of consumers' personal information (PI) for direct marketing is now regulated, and privacy protections extend to unsolicited information, allowing consumers to access and correct PI. The rules on sharing PI with companies outside Australia have also been restricted, sensitive PI (including health related information, DNA and biometric data) is regulated, and the Privacy Commissioner's powers have been enhanced. Credit reporting laws are also affected. The changes went into effect on March 12, 2014.

D. Worldwide Developments in Self-Regulation

- **Self-Regulation Around the World.** Advertising and privacy self-regulation is most advanced in the U.S. Several U.S. organizations, including CARU, offer safe harbor programs approved by the FTC under COPPA. The NAI has managed a self-regulatory program for OBA for many years.

[42] *See* Privacy Amendment (Enhancing Privacy Protection) Act 2012, No. 197, http://www.comlaw.gov.au/Series/C2012A00197.

The NAI code applies only to its members, who include third party network advertisers and others who help deliver and manage third party digital advertising. One provision of the code requires members to include in contracts mechanisms to assure that their clients provide appropriate transparency and choice about receiving OBA-targeted ads. A separate code covering mobile has also been adopted and integration of requirements is occurring this year. A larger coalition that includes members from all aspects of the advertising ecosystem, the DAA, also covers OBA. The DAA accountability program is operated by an arm of the CBBB. Some of the DAA members, including the Direct Marketing Association (DMA), require its members to adhere to the DAA Code.

Industry groups have been promoting self-regulation around the world. The International Chamber of Commerce (ICC) Marketing and Advertising Commission's Code of Marketing and Advertising Practice was updated to include additional provisions on digital marketing and privacy. Implementation of the ICC Code, however, occurs at the national level, and the ICC does not provide a centralized enforcement mechanism. Some privacy self-regulatory bodies, such as TRUSTe, offer EU Safe Harbor programs to address data transfers from the EU, as well as certifications geared to meet the APEC principles. The Internet Advertising Bureau of Europe (IABE) has an OBA self-regulatory program similar to the DAA program in the U.S., but, as noted above, the Article 29 Working Party has said that the opt-out program does not meet EU requirements.

The EU has developed more of a co-regulatory model of "self-regulation" with the government sometimes playing a leading or convening role. This has not been as common in U.S. self-regulatory programs for reasons that have to do with First Amendment rights accorded to speech, including commercial speech, as well as regulatory protections under the Administrative Procedure Act (APA) and other U.S. laws. Nevertheless, we have seen in the U.S. echoes of this co-regulatory approach with efforts to promote multi-stakeholder codes of conduct through NTIA and other initiatives. In some cases groups developing industry codes are issuing them for public comment, but in general the U.S. business view tends to be that industry should try to keep the "self" in "self-regulation."

- **Forced Localization.** The principle of "forced localization" of information and communications technology reflected by German Chancellor Merkel's announcement (see above) is part of a broader trend. While often based on protectionist views of keeping jobs in country, this notion is also gaining traction in additional countries as a result of the NSA disclosures. Investments and policy initiatives to promote local information technology and communications growth are a reality, and many factors that promote such development – including promoting a stable economy, skilled workforce, and robust rule of law – benefit both the state and those who wish to trade with it. But countries such as China, India, and Nigeria are increasingly taking measures such as requiring technology transfers, local sourcing, and the escrow of source code and other sensitive tools. These measures threaten the future of local industries and a country's connection with the larger world, and often appear to be based on protectionist sympathies rather than larger policy objectives.

V. Impact on the Toy Industry

Privacy and data security issues affect the day-to-day operations of toy companies, both in kid-directed and adult-directed offerings. In the U.S., the FTC's COPPA restrictions affect the ability of toy companies to obtain necessary data to analyze their digital offerings and improve content, allow children to enjoy personalized, but anonymous, online experiences, and benefit from the ability to offer targeted advertising on their e-commerce and adult sites. Close attention to technical data collection activities and the actions of third parties are essential to assure that they are consistent with the COPPA rules. Increased focus on mobile privacy, coupled with the growth of mobile device usage by children and dramatic increase in kid-directed mobile apps, explains the increased oversight and enforcement-targeting of companies that lack mobile privacy policies, or that have failed to update them.

Globalization of trade and cross-border sharing of information has led to increased communication and coordination between policymakers to address privacy and data security. Retailer data breaches and revelations of international surveillance by the U.S. and others have also helped drive privacy and cybersecurity to the top of the international agenda, often in ways that are detrimental to businesses in general and U.S. businesses in particular. As new privacy laws are enacted, and those laws restrict data collection from children, the absence of a global framework that establishes common-sense exemptions and protections will become a significantly greater obstacle to toy company advertising and marketing objectives.

There are many examples of how policy developments in one region are affecting developments in others.

For example, the push by consumers to recognize broader rights to access personal data, and to create a "Consumer Privacy Bill of Rights" in the U.S., reflect influence of the EU framework. The goal is to shift to a regime where privacy is considered a fundamental right where consumers, not businesses, have the ability to control data from or about them.

Conversely, the revised EU Privacy Regulation, which includes a broad provision protecting privacy of all minors, shows the influence of United Nations legal instruments defining children to include all minors. This concept is favored by NGOs advocating more extensive limits on advertising and broader privacy protections in the U.S. In particular, the proposed Regulation attempts to apply COPPA-like limits on collection of information from children under 13, but without sensible exclusions and a scaled approach to parental consent. Absent strong action from child-oriented companies and their allies, child-directed websites and online services could be eliminated or drastically curtailed if the proposed EU Regulation goes into effect without key changes and clarifications.

The cross-border effect of U.S. laws on the EU proposal can also be seen in the general limit on collection of personal information from children under 13 absent verifiable parental consent, as well as the data breach notification requirement. Conversely, revisions to the COPPA Rule that expressly define IP addresses and device identifiers as personal information illustrate the impact of changing thinking about just what types of data are "personal," aligning with views in the EU on this point.

Additionally, the FTC applies COPPA to foreign websites that purposefully target U.S. children, an approach also applied by CARU in its privacy self-regulatory actions. The proposed EU Regulation's purported extraterritorial effect goes beyond normal interpretations of the "purposeful targeting" test, however. The EU regulation will therefore likely create significant legal jurisdictional questions of considerable concern, given what appears to be greater scrutiny on U .S. businesses than on practices by European players. With EU privacy law serving as a model for other laws globally, expansion of this concept will likely further complicate business operations as other regions adopt data protection laws and seek recognition by EU authorities of their "adequacy."

VI. Recommended Action

Safeguarding consumer privacy, especially children's privacy, remains a priority for the toy industry. Awareness of applicable rules and strong compliance initiatives are an essential part of industry's responsibilities in an environment of growing scrutiny. TIA engagement in regulatory and self-regulatory initiatives to date has helped advance key goals: supporting appropriate regulation and encouraging requirements and modifications grounded in operational and technical realities that are necessary to advance appropriate business objectives. TIA should continue to closely coordinate with allied trade associations, like the Association of National Advertisers (ANA), DMA, and others, to oppose new restrictions on children's privacy, such as the Do Not Track Kids Act or overly broad restrictions on advertising.

- **COPPA**

  Toy companies recognize the special vulnerabilities of children and have supported COPPA, which has worked effectively to protect children's privacy. The changes adopted by the FTC do impinge on the ability of toy companies to offer creative, fun, and interactive websites that give children an anonymous experience, particularly limits on the collection of videos and photos. Posting of videos and photos now requires full parental consent in all circumstances, creating new administrative burdens to offer a social media experience to children. The proposed Do Not Track Kids Act would impose even more far-reaching restrictions. Recent petitions by NGOs asserting that companies have violated COPPA are not just designed to prod the FTC to take enforcement actions, but also seek to undermine fundamental principles of self-regulation by asserting that self-regulation is ineffective.

  TIA has been actively engaged with the CARU Supporters task force to discuss complicated questions about application and interpretation of COPPA. CARU met with the FTC staff in December 2013 to discuss some of these concerns, and to broaden the dialogue with the FTC staff with an eye toward building trust and having the CARU Supporters be viewed as an important resource for practical issues and questions about application. The goal is to assure that COPPA and the recent Final Rule are interpreted and enforced appropriately and with a view to practical and operational considerations that toy and other children's companies face every day. TIA should continue to seek opportunities to advocate its position with other executive branch and legislative leaders as appropriate, directly and through other umbrella organizations.

- **OBA**

  Under the COPPA Final Rule, OBA on child-directed websites or areas of websites is impermissible. Thus, careful attention must be paid to ensure that any tracking falls within the definition of supporting the internal operations of the website, and is used for permitted analytical or other purposes and not for tracking. Due diligence with analytics and ad-serving firms remains important, as operators are strictly liable for all information collection activities that occur at their site.

- **Online and Mobile Guidance**
  TIA is releasing an updated guidance on COPPA compliance – Dos and Don'ts for Compliance with COPPA – concurrently with this white paper. TIA has also developed a 2014 update to the Toy Industry Checklist for Mobile Apps and Promotions. TIA will continue to update information and guidance materials and welcomes comments and questions on these items, including requests for additional guides and educational materials.

- **Multi-Stakeholder Codes of Conduct**
  TIA did monitor the NTIA multi-stakeholder initiative that resulted in the adoption of a code of conduct for privacy disclosures in apps. The code of conduct has not been widely adopted, and it is not likely that it will be adopted for kid-directed apps since the code has not been recognized by the FTC as meeting the requirements of COPPA. However, NTIA has initiated a new stakeholder dialogue, this time on facial recognition. With new types of gaming platforms available, facial recognition may become a more important technical feature of online games and apps. Consequently, TIA should continue to monitor the NTIA process and provide practical input as the latest multi-stakeholder initiative moves forward.

- **EU**
  The proposed EU Regulation raises the possibility that current web-based marketing to children could be severely restricted, especially if the Commission fails to define verifiable parental consent in a practical way. The notion of an "eraser button" for kids' data has gained favor in Europe, as EU privacy groups already advocate a "right to be forgotten." More broadly, the extraterritorial impact creates significant concerns about potential liability exposure, and practical ways to manage that exposure should the Regulation be finalized with that provision. Given the deep suspicion of U.S. players as a result of NSA and other disclosures, EU toy operations are best positioned to participate. Coordination through organizations such as the Toy Industries of Europe (TIE) and the World Federation of Advertisers (WFA) is the optimal way to try to educate and influence the European Commission on children's advertising issues. However, input from American businesses is vital to assure that there is a thorough understanding of the practical and technical considerations necessary to develop detailed guidance about verifiable parental consent, situations where consent is not required, and various means to obtain consent.

- **Advertising Self-Regulation**
  As data collection is central to all types of digital advertising, the intersection of privacy and advertising policy creates its own set of issues. TIA is working with the CARU Supporters task force to promote some revisions to the CARU Guidelines designed to reflect, but not go beyond, COPPA. From time to time the question arises about whether there is a benefit to the toy industry through promoting the development of a more detailed children's advertising or privacy code, and/or an assessment of the effectiveness of self-regulatory enforcement actions when it comes to children's advertising and privacy. Earlier toy industry efforts to incorporate more detailed children's privacy guidance internationally through the ICC failed largely due to opposition from non-U.S. participants who feared that detailed requirements in the ICC Code could become a baseline for restrictive national legislation in accession and other states. This possibility should be part of any further discussion on the topic.

***

As the global regulatory requirements expand, the M2C subcommittee should discuss further TIA's role in advancing industry objectives. For global marketers, the result of proliferating regulations will be the necessity to adhere to the most stringent standards, a result that will prove costly and could potentially limit the ability to offer content and information. Ongoing advocacy as necessary, member awareness and compliance education, support for self-regulation, and coordination with other organizations will likely remain components of TIA's strategy in managing privacy and advertising challenges.