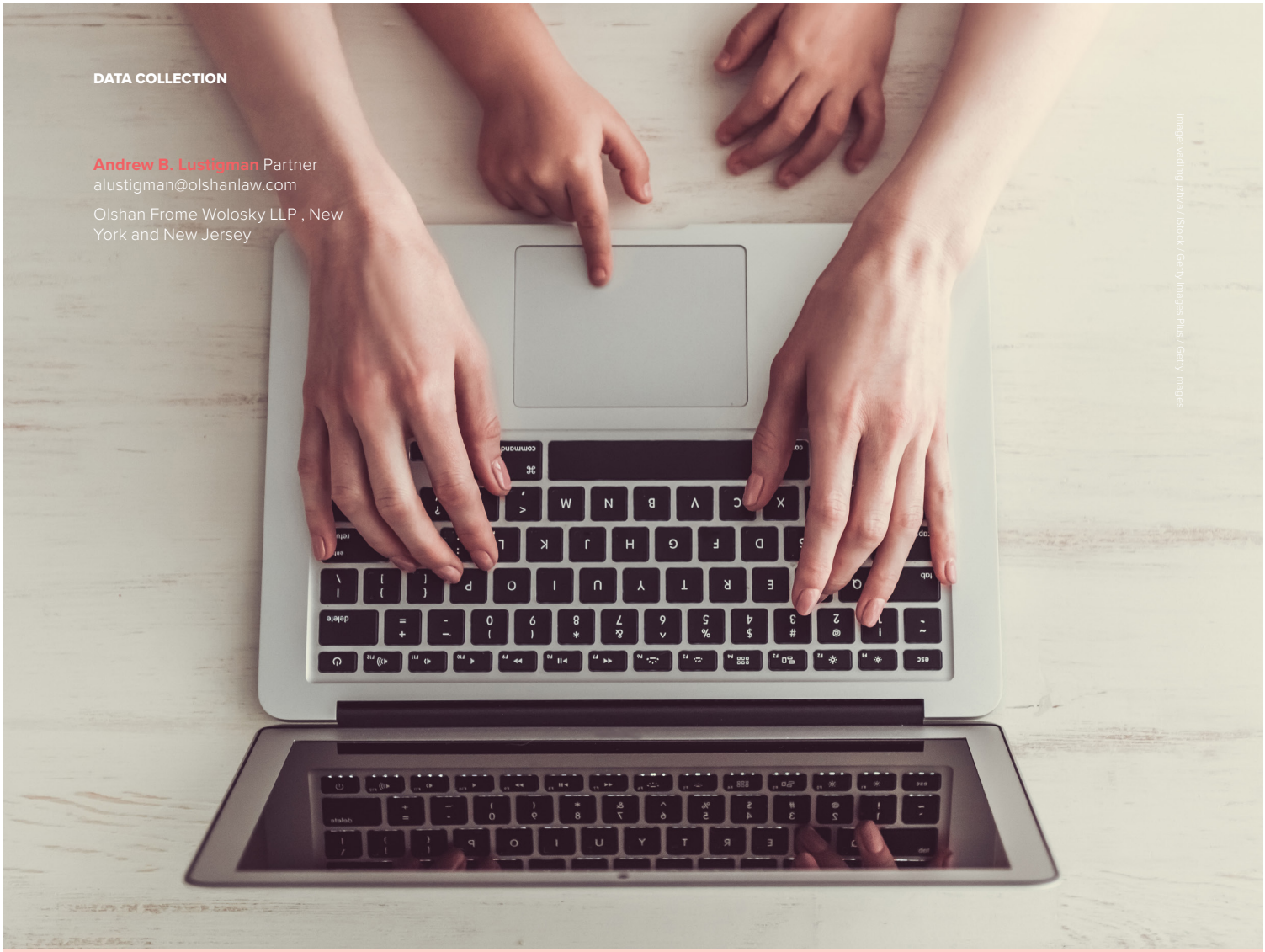

Andrew B. Lustigman Partner
alustigman@olshanlaw.com

Olshan Frome Wolosky LLP , New York and New Jersey

The FTC's COPPA compliance update

Under the US Children's Online Privacy Protection Act ('COPPA'), businesses that collect data from children are subject to strict compliance obligations regarding data collection, sharing, and security. Compliance is critical as the US Federal Trade Commission ('FTC') frequently brings enforcement actions against non-compliant businesses, seeking significant penalties. Reflecting the impact of new technology utilised by children, the FTC has recently updated its six step COPPA compliance plan. The FTC's update seeks to address the ever-evolving effect of new technology on data collection practices and provides new means of obtaining requisite parental consent, as Andrew B. Lustigman of Olshan Frome Wolosky LLP explains.

What is COPPA?

COPPA governs the collection, sharing and security of online personal information from children under the age of 13. Under COPPA, the FTC has promulgated regulations known as the Children's Online Privacy Protection Rule (16 CFR Part 312). The FTC has been aggressive in enforcing COPPA against online businesses, obtaining large penalties and issuing press releases that are widely picked up by news agencies. COPPA applies to websites or online services that are reasonably found to be directed at children. COPPA also applies to general audience websites or online services with actual knowledge that they are collecting, using or disclosing personal information from children under 13. For such general audience websites, the FTC requires that businesses comply with the parental consent for those children or otherwise age-gate to exclude children. In such instances, among other things, parental consent is required before collecting or permitting such access. Even if a technology is found to be potentially subject to COPPA, it still only applies to the online collection of 'personal information' from a child. Personal information, however, is broadly defined. It includes individually identifiable information about a child, such as first and last name, address or geolocation information, online contact information (email address, video chat identifier, IM identifier), a screen name, telephone number, social security number, persistent online identifiers that can be used to recognise a user over time and across different sites

continued

(such as cookies), and visual or audio recordings of a child's voice or image. Online collection is also broadly defined to include not just online tracking or actual collection but providing children with access to publicly disclose personal information either through an electronic communication or posting.

Compliance plan update

Under the Rule, subject businesses should follow the FTC's six step compliance plan to ensure that only permissible information is collected with appropriate parental consent and is otherwise appropriately protected. There are three key updates to the six step plan. First, the updated compliance plan addresses the advancing way in which companies are collecting personal information from children. The updated compliance plan expands to new business models that are collecting data through less traditional channels. For example, the updated plan suggests that the use of voice-activated devices to collect personal information may trigger COPPA compliance obligations.

Second, the updated compliance plan expands its definition of what technology is covered by COPPA. Previously, COPPA focused the majority of its compliance power on businesses' collection of children's personal information on websites and through personal apps. The FTC has now made it clear that COPPA also applies to connected toys and devices marketed to children that collect personal information, including voice recordings and geographical location.

Third, the FTC has updated the methods by which businesses may obtain the requisite parental consent prior to collecting personal information from their children under the age of 13. Adding to the list of methods that includes obtaining a signed consent form and having the parent call a toll-free number staffed by trained personnel, the FTC has suggested two additional acceptable methods that businesses may use to obtain parental consent. Businesses may now obtain consent by asking a series of knowledge-based challenge questions that would be difficult for someone other than a parent to answer, or by using facial recognition technology to identify the parent. We briefly explore these updates as part of the overall updated six step compliance plan.

Step one: is the technology subject to COPPA?

As COPPA applies only to certain online collection of personal information from children under 13, it is important to first determine if COPPA is potentially triggered. As discussed above, COPPA compliance obligations will be triggered if the online technology is directed to children under 13 and personal information is collected either by the company or third parties (like an animated children's game), or the online technology is directed at a general audience but the business has actual knowledge that personal information is collected from children under 13. This category presents the greatest trap, as many online companies do not expect (or necessarily want) users under the age of 13. Examples can include websites and apps focused on music or entertainment, or social media platforms. An additional category can include an advertising network or plug-in and there is actual knowledge that personal information from users of a website or service directed to children under 13 is being collected. Keep in mind that the Rule covers a broad array of technology, including mobile apps (including social media and game apps), gaming platforms, plug-ins, location services, VOIP, connected toys and other connected devices.

Step two: privacy policy disclosures

Assuming COPPA compliance obligations are triggered, the online technology is required to clearly and comprehensively disclose how personal information from children is handled. The notice, typically a privacy policy, must describe the online technology companies' practices, as well as those who are collecting such data on the website or platform, such as an advertising network. While there is no form privacy policy, the disclosure must include the name and contact information of all operators that are collecting or maintaining the childrens' personal information, the type of personal information being collected, how it is being collected, how it will be used internally and with third parties, and a description of parental rights. The parental rights section must tell parents how they can review their child's personal information, and how to direct such information be deleted or collection ceased.

Step three: Prior parental notification

In addition to posting a privacy policy, a subject business must directly notify parents about its data collection practices before collecting COPPA-covered personal information. The notice must tell parents, among other things, that the technology wants to collect personal information about their child, the information that is being collected and shared, that parental consent is required and how it is to be given, a link to the privacy policy, how the parent can give their consent, and that if the parent fails to consent within a reasonable period of time, the parent's online contact information will be deleted from its records.

Step 4: Obtaining verifiable parental consent

COPPA requires that a subject business obtain the parent's verifiable consent before collecting, using, or disclosing a child's personal information. Similar to other disclosures, there is flexibility in the method of obtaining the consent. These methods can include obtaining a signed consent form, requiring the use of a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder; calling a toll-free number staffed by trained personnel; or requiring the answer to a reasonable number of dynamic multiple choice

questions with an adequate number of possible answers such that the probability of correctly guessing the answers could not reasonably be achieved by children. Finally, the FTC now allows using facial recognition technology to identify the parent.

Step 5: Honouring parental data collection rights

Consistent with the privacy policy representations, a subject business must respect parents' exercise of their ongoing rights. That means that if a parent requests, the business must provide the parent with the ability to review the personal information collected about their child, provide a means to revoke consent and block future collection, and delete the data.

Step 6: Reasonable data security

COPPA requires subject businesses to establish and maintain reasonable procedures to protect the confidentiality and integrity of the information collected from children. The best place to start is to only collect the least amount of information necessary and to securely delete that information once it is no longer needed. Businesses need to continually confirm that not only are their servers secure, but that any party with which it shares information is similarly capable of maintaining its confidentiality, security and integrity.

Conclusion

The FTC's recent updates to its COPPA compliance plan attempt to address the increasing impact of technology on the data collection practices of businesses that collect information from children. Businesses in the practice of collecting personal information from users should look closely as to whether their technology is receiving personal information from children, even if it is from sources not traditionally thought of as a website or an app directed at children. If there is the potential that the online activity is subject to COPPA, the business should carefully complete the six step compliance plan and confirm that it is sufficiently addressing its compliance obligations.

CMA launches an investigation into price comparison website

The UK's Competition and Markets Authority ('CMA') published its final report following its year-long market study into the use of price comparison websites and other apps on 26 September 2017, which sets out recommendations for price comparison websites to ensure that the issues identified are addressed, the majority of which are consumer protection related, as well as launching an investigation into how one price comparison website, which is not identified by the CMA, has set up its contracts with insurers, due to suspicions that the use of retail most favoured nation clauses may have resulted in higher prices for home insurance.

"From a competition law perspective, the most notable development is the CMA's decision to open an investigation into the use of retail most favoured nation clauses by a price comparison website," said Paul Stone, Partner at Charles Russell Speechlys LLP. "The CMA has considered these clauses in other cases but has never reached an infringement finding. It will be interesting to see whether the case proceeds to a final decision or ends with a case closure or commitments."

The overview to the final report explains that an increasing number of people use digital comparison tools, a term used to cover price comparison websites and other intermediary services used by consumers to compare products or services from a range of businesses, and that such tools "are mostly a force for good: they make it easier for people to shop around, and improve competition - which is a spur to lower prices, higher quality, innovation and efficiency." However, the report explains that more can be done to ensure that the benefits are felt as widely as possible and as such the CMA is taking steps and recommending other action by companies, regulators and the Government to make sure that improvements happen.

The CMA's press release accompanying the final report lists what it deems to be the main recommendations put forward in the report, which includes that all sites should follow the CMA's ground rules in that they should be clear, accurate, responsible and easy to use; that all sites should be clear about how they make money, how many deals they are displaying and how they are ordering the results; that all sites should be clear on how they protect personal information and how people can control such use; that it should be made as easy as possible for people to make effective comparisons or use different sites; and that all regulators with a stake in this area should work together to ensure people are well protected.

"While the impact of the study will vary by sector, and will also depend on the extent to which companies voluntarily adapt their practice, it is notable that the CMA is combining its wider recommendations with enforcement action," concludes Becket McGrath, Partner at Cooley (UK) LLP. "The compatibility of most favoured nation clauses with competition law in other contexts has been a hotly-contested issue over recent years and it will be interesting to see how this case develops. It is unclear why only one firm has been singled out for investigation but inevitably other sites that use these clauses will be undertaking their own risk assessments. The CMA is presumably hoping that sites will also be considering their use of other clauses that the CMA has identified as potentially problematic, while not yet justifying investigations."