Proskauer

The Future of the FTC: Part I

Proskauer on Privacy Blog on **February 24, 2021**

On January 21, 2021, President Biden designated Federal Trade Commission (the "FTC") Commissioner Rebecca Kelly Slaughter as acting chair of the FTC. Soon thereafter in one of her first speeches in her new role, Chairwoman Slaughter announced two substantive areas of priority for the FTC – the COVID-19 pandemic and racial equity.

The COVID-19 Pandemic

Chairwoman Slaughter noted that the FTC will play an important role in solving pandemic-induced privacy and security issues and identified two sub issues in particular that the FTC will pursue.

Education Technology

First, the pandemic has led to a surge in distance learning. The FTC has power to enforce privacy in the education technology ("ed tech") space through authority conferred by the Children's Online Privacy Protection Act ("COPPA"). COPPA generally requires commercial websites and online services, including mobile applications, aimed at children, or that have actual knowledge that they are collecting personal information from a child, to obtain parental consent before collecting or using personal information from children under the age of 13. In the educational context, schools can consent on behalf of parents to the collection of student's personal information if the information is used only for a school-authorized educational purpose. To receive consent from the school, ed tech services must provide the school with notice of their data collection and use practices.

FTC Guidance

Even if students using an ed tech service are 13 years old or older and not technically covered by COPPA, the service should not use less care or engage in different practices than it would if the users were younger than 13. Further, as a best practice, ed tech services should make notice of its data collection and use practices available to parents and allow parents to review the information collected.

Moreover, while COPPA does not impose obligations directly on schools, schools or school districts engaging in remote learning should consult with their attorneys and information security specialists to review the privacy and security policies of the ed tech services they use and ensure they are appropriate. Schools or school districts should ask potential services:

1. What type of personal information is collected from students?
2. How is personal information used and/or shared?
3. Are schools able to review and delete the information collected from their students? If no, the school cannot consent on the parent's behalf.
4. What measures does the service use to protect the security, confidentiality, and integrity of the personal information collected?
5. What are the service's data retention and deletion policies for children's personal information?

Once schools or school districts have provided consent to a service on behalf of their student's parents, the schools or school districts should provide parents with notice of such consent.

Health Applications

Second, the pandemic has led to an increase in the usage of health applications in place of in-person doctors' visits. In fact, the FTC recently proposed a settlement in its first health application case. The FTC alleged that Flo Health, Inc. ("Flo"), the creator of the Flo Period & Ovulation Tracker, a mobile application that functions as an ovulation calendar, period tracker, and pregnancy guide, promised to keep application users' health data private and only use it to provide the application's services to users. However, according to the FTC, Flo disclosed health data from millions of the application's users to third parties that provided marketing and analytics services to the application. "As part of the proposed settlement, Flo is prohibited from misrepresenting the purposes for which it or entities to whom it discloses data collect, maintain, use, or disclose the data; how much consumers can control these data uses; its compliance with any privacy, security, or compliance program; and how it collects, maintains, uses, discloses, deletes, or protects users' personal information. In addition, Flo must notify affected users about the disclosure of their personal information and instruct any third party that received users' health information to destroy that data."

FTC Guidance

The FTC's guidance for health application developers can be narrowed down to eight key recommendations.

1. Minimize data collected and maintained, and keep data in a de-identified form such that it cannot be reasonably associated with a particular individual.
2. Limit the application's access to information on the user's device. For instance, if an application allows its users to share updates with other users, set the sharing default choice to "private," rather than "public," and allow users to choose who they share their information with.
3. Implement authentication and password requirements to ensure the person accessing a particular account is the legitimate owner of the account, and store passwords securely.
4. Ensure that if the application uses a third-party service provider, mobile platform or code, the third party protects consumer's data and does not have any known security vulnerabilities.
5. Develop a culture of security at the company whereby data security is incorporated into every stage of the application's lifecycle, including design, development, launch, and post-market. Use strong encryption for collected health information, take steps to protect the application from known and future vulnerabilities, and keep track of collected and retained data.
6. Take advantage of pre-existing tools to implement appropriate data and privacy safeguards and stay informed of the latest security vulnerabilities.
7. Implement an accessible privacy policy to tell users what information the application collects and how the company uses, shares, and secures that information.
8. Consider applicable laws, such as the FTC Act, the FTC's Health Breach Notification Rule, the Health Insurance Portability and Accountability Act (HIPAA), the Federal Food, Drug & Cosmetic Act, the COPPA Rule, and the Gramm-Leach-Bliley Act's Safeguards and Privacy Rules.

The Future of the FTC

Chairwoman Slaughter astutely noted that “[a]s businesses, schools, governments, and communities have struggled to find new models for staying open, providing critical services, and keeping in touch, the importance of reliable Internet has grown.” In light of the expansion of the ed tech industry during the pandemic, the FTC is reviewing COPPA to clarify how COPPA applies to the ed tech space. In addition, Chairwoman Slaughter stated that she would like the FTC to pursue more cases like *Flo* and issue a report on broadband privacy practices to provide the public with transparency regarding privacy on the Internet.

Continue to watch this space for developments. A future post will discuss Chairwoman Slaughter’s second priority – racial equity.

View Original

Related Professionals

- **Brooke G. Gottlieb**
  Assistant General Counsel