August 18, 2014

Introduction

In its August 1st report entitled "What's the Deal — An FTC Study on Mobile Shopping Apps," the FTC provides guidance on various disclosures that should be made by mobile apps along with reinforcing a number of prior recommendations related to such apps. Though the staff authors tried to include several positive points (e.g., "[t]he number of readily available privacy policies addressing the collection, use, and sharing of data is a step in the right direction"), the report mostly paints a bleak picture of a marketplace in which companies are not doing enough to inform consumers about the material terms and risks of mobile shopping services.

The core message reduces down to three recommendations for companies and two recommendations for consumers. **The FTC advises that:**

- **Prior to use of a mobile app, companies should disclose to consumers their rights when unauthorized, fraudulent, or erroneous transactions occur**. Many apps tested provided no liability disclosures, while others "placed all liability for unauthorized charges on the consumer." The FTC felt that consumers need to know their potential liability, available protections, and dispute resolution mechanisms, all PRIOR to commitment to use the payment service.
- **Companies should clearly describe how consumer data is used.** Most policies reviewed by the FTC "used vague terms, reserving broad rights to collect, use, and share consumer data without explaining how the apps actually handle consumers' information." Instead, the FTC thinks detailed explanations of companies' actual practices for collecting and using data would be more helpful to consumers in making purchase decisions.
- **Companies should support strong data security *promises* with strong data security *practices***. Although several apps reviewed by the FTC contained the typical technical/organizational/physical security promises, concerns persist that companies aren't actually putting practices in place that properly protect consumer data.

For consumers, the FTC recommends that:

- **Consumers find out what dispute resolution procedures and liability limits apply to a mobile payment app before they begin to use it**, "and consider the payment methods used to fund their purchases." Consumers need to understand where Federal law limits their liability for unauthorized transactions (credit or debit cards) and where it doesn't (prepaid cards or accounts). If consumers cannot find information about the dispute resolution procedures and liability limits of an in-store purchase app prior to download, they should consider downloading an alternative app, or making only small-dollar purchases.
- **Consumers should seek information before they download apps about how their data will be collected, used, and shared**. If this information isn't available or not reassuring, the FTC recommends that consumers consider a different app or limit how they will use the app.

Discussion

The FTC based the above recommendations on a fairly comprehensive analysis of mobile shopping apps. A total of 121 unique apps were surveyed with 60 being from Google Play and 61 from iTunes. The apps were broken down into three categories — price comparison apps (which utilize the cameras resident on the devices to scan barcodes and then perform comparisons of prices across different brands and stores), deal apps (which provide discounts redeemable at physical stores), and in-store purchase apps (which allow actual in-store purchases to be made via the mobile device).

Building on earlier workshops, reports, and enforcement actions, the FTC authors emphasized the continuing need for transparency in the data practices of companies. Their research shows that the batch of mobile apps that they tested clearly lacks the desired transparency. The analysis of the apps performed by the FTC focused on two overarching areas: (1) liability limits and dispute resolution, and (2) privacy and security. This led to several detailed recommendations that build on the general ones above, including:

- Terms and conditions must be made available before using a mobile payment service, particularly in the case of stored value payments (where statutory and contractual liability limits for unauthorized credit or debit card payments don't apply).
- Because mobile devices are more personal as to a particular consumer, more data about that consumer can be collected and shared. Privacy policies for mobile apps (perhaps even more so than with traditional websites) should be abundantly clear about data collection, data use, and data sharing.
- Privacy policies for mobile apps must contain unambiguous and precisely scoped language, clearly indicating what data will be collected and how it will be used.
- Security over the collected consumer data and the transactions conducted with a mobile device must be appropriate given the threats. This view is consistent with the work within NIST in developing the Cybersecurity Framework.

Conclusions

Ultimately, the FTC wants companies to act more responsibly with respect to mobile apps, particularly in the areas of mobile payments and data security. Although the FTC's recommendations are advisory in nature and are not "black letter rules," the report seems to signal the FTC staff's growing frustration with the lack of transparency in the mobile payment/shopping space and no one should be surprised if the FTC steps up its enforcement activity in these areas. Complying with the FTC's calls for clearer disclosures can pose difficult challenges for companies that have to balance the FTC's exhortations for greater transparency against the need for terms that are flexible enough to accommodate continual changes to their business models. Cooley lawyers are experienced in helping clients navigate these tricky waters.

Key Contacts

Adam Ruttenberg **Washington, DC**	**aruttenberg@cooley.com** **+1 202 842 7804**
Scott Dailard San Diego	sdailard@cooley.com +1 858 550 6062
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090