Bloomberg BNA

Electronic Commerce & Law Report™

INTERNET OF THINGS

The authors discuss the emerging technology behind the Internet of Things and the difficulty of creating enforceable terms of services for IoT devices. They discuss options outlined in the Federal Trade Commission's recent IoT report and then propose some solutions of their own.

The Next Big Thing: Enforcing Terms of Service in an Internet of Things World

By Jesse M. Brody and Donna L. Wilson

While a universally accepted definition of the Internet of Things (IoT) does not yet exist, the phrase has been coined to refer to the ability of everyday objects to connect to the Internet and to send and receive data. Thus, we are not far from living in a world where every device — from the tiny sensors on your doors and windows to the largest home appliances — has Internet capability that renders it not only uniquely identifiable, but accessible from anywhere you have Internet access.

Examples of IoT products include smart appliances, vehicle-to-vehicle technology, health monitoring devices, drones and smart utility grids. Although some of these examples are either currently in use or in development, the future looks to bring many variations and applications of the IoT.

The Federal Trade Commission (FTC) has even recently jumped on the IoT bandwagon, releasing a report (the ''IoT Report'')[1] in January 2015 calling on companies that develop IoT connected devices to take proactive steps to protect consumers' privacy and keep their data secure. Thus, a few of the key IoT legal issues to watch include privacy, data security, ownership of data (including the use of aggregated data), and responsibility and product liability for when a ''thing'' fails or when one thing causes another thing to fail.

In terms of reducing a company's risk of legal liability arising out of an IoT product, product manufacturers will likely start looking for ways to enforce their standard ''website'' or ''mobile app'' terms of service (or terms of use) (''ToS'') against consumer IoT product purchasers. Each ToS will inevitably include clauses that not only limit the company's liability but will include arbitration clauses (typically combined with class action waiver language) in an attempt to reduce the risk of class action lawsuits being brought for product defects and other potential privacy and data security-related claims in the event of a data security breach.

Thus, a question arises as to how an IoT product manufacturer will go about obtaining an agreement to a ToS from its consumer purchaser that will be enforceable against that consumer as well as any other individuals who happen to use that IoT device at a later day after its initial purchase. For instance, think of an appliance that is purchased by one family member but is ultimately used by many individuals throughout the product's lifetime.

Jesse Brody is a partner in both the Privacy & Data Security and Advertising, Marketing & Media practice groups at the law firm of Manatt Phelps & Phillips LLP in the Los Angeles office. Mr. Brody is accredited by the International Association of Privacy Professionals as a Certified Information Privacy Professional. He can be reached at jbrody@manatt.com.

Donna Wilson is a partner at the law firm of Manatt Phelps & Phillips LLP in the Los Angeles office. Donna co-chairs Manatt's Privacy & Data Security practice group. Shecan be reached at dlwilson@manatt.com.

[1] ''Internet of Things: Privacy & Security in a Connected World,'' FTC Staff Report, January 2015 (available at: http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf) (20 ECLR 179, 2/4/15).

 ISSN 1098-5190

As an initial matter, many IoT product manufacturers may believe that consumer contracting issues can be fully addressed at the point of sale. For example, shrink-wrap contracts entered widespread use in the 1980s and 1990s. Many of the leading cases regarding contracts that contain additional terms after the purchase of the products were developed in connection with software purchases.

Due to space limitations, the only way to include all of the terms of a contract was to separate some of the terms and enclose them within the packaging. Even though required elements of contract formation were missing, such as notice of the terms, and mutual assent thereto, courts slowly came to accept shrink-wrap contracts provided that the customer was able to return the product within a reasonable period of time.

In *ProCD v. Zeidenberg*,[2] the Seventh Circuit held that Zeidenberg was bound by the terms and conditions of a software license included in a users' manual within the packaging, and which was displayed on a computer screen upon installation and use of the software. The Seventh Circuit held that ''[Shrink-wrap] licenses are enforceable unless their terms are objectionable on grounds applicable to contracts in general.''[3]

However, an IoT device manufacturer may not be wise to rely solely on a shrink-wrap contract formation process with its customer. There will often be circumstances where it will want to obtain an agreement to a ToS with individuals beyond the product's original purchaser — such as in instances in which the user or the product is not the purchaser of the IoT device or where multiple individuals in the product's lifespan will use the IoT device. In the instance of a smart meter or a connected car, for example, all family members of a home may use the product, even though potentially only one member of the family made the original purchase.

Thus, in many instances in the IoT device context due to the risk of liability arising out of the company's misuse of information collected or the potential for breaches of data security, it is likely that manufacturers will want to rely on an electronic agreement to a ToS that was obtained in a way to bind all potential users of an IoT device instead of (or in addition to) the traditional shrink-wrap agreement.

FTC Report Provides Guidance on Acceptance.

As part of the IoT Report the FTC gave us some hints on how IoT product manufacturers may attempt to get an electronic agreement to legal terms in its discussion addressing the notion of giving consumer notice and choice when a company will collect and use data from an IoT device in ways a consumer might not expect. The FTC provides examples of how companies can provide notice and provide choices on connected devices, especially when there is no consumer interface. These examples included (among others):

- providing choices at the time of purchase,
- providing video tutorials that explain how to manage privacy settings,
- affixing a QR code or similar barcode that, when scanned, would take the consumer to a website with information about the applicable data practice,
- providing choices during setup, for example as part of a setup wizard,
- using command centers or dashboards, and
- ''Out of Band'' communications requested by consumers, such as allowing users to receive information through e-mails or texts.

Shrink-wrap, Browse-wrap and Click-wrap Agreements.

While these examples from the IoT Report are quite useful for purposes of providing notice and choice in the privacy context, they may also independently serve as ways that companies may choose to obtain an electronic agreement from all users of an IoT device to a ToS. We could also envision additional scenarios for obtaining an agreement to a ToS for IoT products that have a product warranty associated with them whereby the documentation provided in the product packaging directs the consumers to a traditional website where during the sign-up process a company could obtain assent to a ToS, but this process still leaves out all the potential users of the IoT product that fail to sign up for the product warranty.

Also, IoT products with associated websites or mobile apps that are required to be used in order to gain the benefits of the IoT product present easy opportunities to obtain an agreement to a ToS in the traditional electronic click-wrap manner discussed in more detail below.

Also, while privacy disclosures are typically made in notice form, a ToS may only be found to be enforceable against a consumer if a proper electronic agreement is entered into with an individual that meets the requirements of the Electronic Signatures in Global and National Commerce Act (commonly known as ''E-SIGN'').[4] As background, obtaining an agreement to a ToS in the online context generally exists in two forms: (i) ''click-wrap'' and (ii) ''browse-wrap.'' With click-wrap agreements, users must provide express agreement or assent to online agreements by clicking ''I agree'' and actively checking an unchecked box, or performing some other affirmative action that meets the requirements of E-SIGN.

Most times, a hyperlink to the text of the agreement is next to an ''I agree'' button, or in some cases, users are required to scroll through the terms of an online agreement prior to clicking ''I agree.''

By contrast, with browse-wrap agreements, no affirmative action is required by users. Rather, a link to the online agreement is passively placed somewhere on the website (usually at the bottom of a page), and users have the option to read the agreement but are not required to do so before they can browse the website or use the services provided therein. Typically, browse-wrap agreements contain clauses stating that a user's use of the website or the website's services constitutes assent to the terms of the agreement.

[2] *ProCD v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996) (1 ECLR 298, 6/28/96).

[3] *Id*. at 1448.

[4] Electronic Signatures in Global and National Commerce Act (''E-SIGN''), 15 U.S.C. 7001 et seq., effective October 1, 2000.

   ISSN 1098-5190

Recently, in a high-profile case addressing the issue of whether a browse-wrap agreement by itself results in an enforceable electronic agreement, the Ninth Circuit in *Nguyen v. Barnes & Noble Inc.*[5] held that the presence of hyperlinks directing users to a website's ToS alone (even when in close proximity to buttons on which users must click, such as a ''checkout'' button) — without more — was insufficient to give constructive notice to users of those ToS.

In light of this lack of notice, the Ninth Circuit held Barnes & Noble's arbitration provision was unenforceable due to the absence of users' express agreement to the online ToS. Thus, browse-wrap agreements are typically only enforced when there is evidence that users have actual or constructive notice of their terms, leaving companies that rely on them in a precarious position when they try to enforce their ToS since these issues of actual and constructive notice will ultimately be left up to courts to decide.

In the IoT product context, companies interested in ensuring that they enter into enforceable agreements with their consumer purchasers will need to impress upon their technology developers the importance of building in capabilities that allow for acceptance of relevant legal terms by multiple device users. Thus, IoT product developers will need to be creative in figuring out ways to incorporate functionality that will not only give consumers notice and choice for data collection for privacy compliance (as discussed in the FTC IoT Report) but that also includes functionality that is similar to or the equivalent of the click-wrap agreement process incorporated on many websites today.

[5] *Nguyen v. Barnes &Noble Inc.*, 763 F.3d 1171 (9th Cir. 2014) (19 ECLR 1076, 8/27/14).

Finally, when designing a click-wrap-like process for an IoT product, it is important to keep in mind that the following steps can further strengthen a click-wrap agreement to make them more consumer-friendly and thus help with enforceability:

- Layer agreements with notice of the most material and unexpected terms highlighted upfront.
- Maintain records of user acceptance.
- Allow users to print, or especially in the IoT context, e-mail or otherwise send themselves the full ToS.

Conclusion

The Ninth Circuit's decision in *Nguyen* illustrates that in order for terms and conditions to be enforceable, regardless of whether we are talking online or another context, a company must not only ensure that the ToS appears conspicuously but also obtain individual assent to those terms in a manner that complies with E-SIGN.

When developing and launching an IoT product, presenting a ToS in a conspicuous manner and obtaining assent to legal terms will be challenging, especially for those products that don't have screens so that a consumer can easily review and check a box in order to agree to a company's ToS. Also, the issue of downstream IoT product users who don't agree to the ToS at time of product purchase or setup can raise interesting issues of enforceability if each ultimate user of an IoT product has not assented to the ToS.

Companies that are developing IoT products and who wish to limit their liability and avoid class action lawsuits are well advised to have their product developers work directly with legal experts who can develop consumer contacting processes that will result in enforceable agreements with their customers.