What You Need to Tell Your Clients About Their Website and Mobile App

By Adam D.H. Grant, Esq.

Virtually every one of our clients have carved out their niche in the digital diaspora we call the World Wide Web and some have ventured into the unknown by relying on mobile apps. However, what they don't know about digital privacy in this brave new world will hurt them. Some clients merely use their websites and mobile apps to provide information, but if your website or app includes a "contact us" page that allows the users to provide their name and address, then your clients are collecting "personal identifiable information," otherwise known as PII, and now have obligations to the user they never dreamed about. Below is what you need to tell your clients about their website and mobile app.

At the heart of digital privacy is safeguarding a person's personal identifiable information, but the problem is defining PII

What is personal identifiable information?

At the heart of digital privacy is safeguarding a person's personal identifiable information, but the problem is defining PII. It seems like a simple question, but depending on where you go to look, the answer is not so simple. The obvious answers include name, address, online contact information, telephone number, and social security number. Title 16, Chapter I, Subchapter C, Part 312.2 However, the not so obvious includes a "persistent identifier," a customer number held in a cookie; an Internet Protocol (IP) address, a unique device identifier; and "geolocation," locating where your computer or phone is using GPS. *Id*. Additionally, as of July 1, 2015, Assembly Bill 179 amended Nevada Revised Statutes section 603A.040, which defines Nevada's laws on the security of personal information, to include driver authorization card numbers, medical or health insurance ID numbers, unique identifiers, or e-mail addresses, in combination with passwords, access codes, or security questions and answers that would permit access to an online account. There are many other variations in virtually every state in the country.

Select federal laws you should consider

With children frequently using mobile apps on their phones, the Children's Online Privacy Protection Act ("COPPA"), 156 U.S.C. §§ 6501–6505, helps protect children under 13 years old when visiting websites or online services directed to them or when such websites or services have actual knowledge they are collecting PII online from such a child. So, if your client's website or mobile app is directed at children or children use the site or mobile app and put in their PII, then your client has significant obligations. If your client's website or mobile app is used by children, then your client must obtain parental consent and take reasonable steps to notify the parent regarding the collection, use, or disclosure of the information. Your service must also include a means by which the parent can provide verifiable consent. In addition to this direct notice, the law requires the website or app to post a prominent and clearly labeled link to an online notice of its information practices with regard to children on the home or landing page screen. The parent must also have the right to review the personal information provided by the child. Under certain circumstances, your client can fall within a safe harbor program by providing a proposal for a self-regulatory program and report on themselves to the Federal Trade Commission (FTC) each year. Your client will need to maintain the underlying documentation for at least three years and make the information available to the FTC for inspection and copying. The law provides for enforcement under the FTC Act, 15 U.S.C. § 57a(a)(1)(B), and a violation would be deemed an unfair or deceptive act or practice pursuant to section 18(a)(1(B) of the Act.

Advising your client what they should expect if the FTC finds they violated the disclosure requirements should be a top priority. The FTC commonly takes one of two routes in enforcement. Consider the May 10, 2016 announcement by the FTC that it approved a final order resolving its complaint against Vulcun, a popular Web browser game, in which it alleged Vulcun installed an application on consumer's mo-

bile devices without their permission. *See* https://www.ftc.gov/news-events/press-releases/2016/05/ftc-approves-final-order-vulcun-deceptive-app-installation-case. Under the terms of the order, Vulcun is required to modify its app to disclose what it intends to do, to obtain consent, and to prevent Vulcun from misrepresenting certain aspects of its app. On the other hand, the FTC required a company owned by Walt Disney to pay $3 million for collecting children's personal information without their parents' consent.

The Federal Trade Commission can help

Sometimes going to the source is the best place to start. The Federal Trade Commission's website is full of amazing source information and up to do date commission opinions. On October 25, 2016, the FTC published an amazing guide for business. The guide can be downloaded for free at https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business. The guide has excellent tips you can pass on to your client. For example, (1) don't collect personal information if you don't need it; (2) hold on to the information only as long as you need it for your business; and (3) don't use personal information when it's not necessary. These all seem logical and simple, but in this age of big data, most of your client's are doing things they don't need to do and keeping the information longer than they need it, simply because it is too difficult to undo what has been done.

The FTC also addressed the expanding use of smartphones and social media when it made its recommendations as to how a business can make effective disclosures in digital advertising. The FTC published its guidelines on its website and can be reviewed at https://www.ftc.gov/news-events/press-releases/2013/03/ftc-staff-revises-online-advertising-disclosure-guidelines. The FTC also published an excellent video providing very specific tips for mobile app developers. See https://www.ftc.gov/news-events/press-releases/2013/03/ftc-announces-video-tips-mobile-app-developers).

Compliance without insanity

Virtually every state has privacy laws and compliance with all is almost impossible. Advising your client to adhere to federal law and engage in best practices will allow them to at least get some sleep at night.

Adam D.H. Grant is a shareholder with Alpert, Barr & Grant and whose 26 year practice includes a focus on mobile app and digital privacy.

BAR SERVICES

Live CLE Seminars

Ethics in Government Law
—a special presentation at CCBA's Janaury Luncheon!

Learn about the provisions of the Ethics in Government Law set forth in NRS 281A!

Speaker: Yvonne M. Nevarez-Goodson, Esq., Executive Director of the Nevada Commission on Ethics
Date: Thursday, January 26, 2017
Time: 12:00 p.m. to 1:30 p.m.
Location: Vic & Anthony's Steakhouse @ Golden Nugget
Credits: 1 Ethics CLE Credits for Nevada lawyers

RSVP w/payment & entree selection to CCBA by Friday, January 20, 2017. For more details, see page 48.

Cyber Fraud & Attacks: What You Need to Do & Know!

Learn about concerns related to digital data, applicable federal and state laws related to security breach notices, and tips for avoiding data breach problems!

Speaker: Adam D. H. Grant, Esq. from Alpert, Barr, & Grant
Date: Friday, February 3, 2017
Lunch: 11:30 a.m. to 12:00 p.m.
Program: 12:00 to 1:30 p.m.
Location: Depo International, 703 S. 8th Street, Las Vegas, NV
Credits: 1.5 General CLE Credits for Nevada lawyers
BONUS: This event includes .5 General CLE Credit FREE for CCBA Members and FREE lunch sponsored by Alpert Barr & Grant for all registered attendees!

CCBA CLE Programming Sponsors: