Developments Generating Demand for Privacy and Data Security Legal Practice

The Internet of Things and emerging technologies, cross-device tracking, data security, state attorney general enforcement and privacy legislation around the world (including the EU and Canada) are all helping ensure that 2017 will be another busy year for privacy and data security lawyers.

Specific examples of areas that are generating demand for expert legal interpretation and guidance include:

- **The Internet of Things and emerging technologies.** The days when internet connectivity was strictly between an individual and his or her device screen are over. Now our "things" are sending and receiving data over the internet. This has caught the attention of regulators. In February 2016, ASUSTeK Computer settled a Federal Trade Commission (FTC) enforcement action regarding security flaws in its routers. A February 2017 settlement by Vizio with the FTC and New Jersey Attorney General regarding smart television tracking demonstrates the application of established consumer protection principles to emerging technologies. In a blog post about this settlement, the FTC noted its guidance in Careful Connections: Building Security in the Internet of Things.
- **Cross-device tracking.** Cross-device tracking occurs when platforms, publishers, and ad technology companies connect consumers' activities across their smartphones, tablets, desktop computers, and other connected devices. In January 2017, the Federal Trade Commission issued a staff report on cross-device tracking that recommends that companies engaged in cross-device tracking: (1) be transparent about their data collection and use practices; (2) provide choice mechanisms that give consumers control over their data; (3) provide heightened protections for sensitive information, including health, financial, and children's information; and (4) maintain reasonable security of collected data.
- **Data security**. The Federal Trade Commission (FTC) and state attorneys general continue to enforce data security. Companies need to implement cybersecurity measures consistent with applicable federal and state data security standards and frameworks, including Section 5 of the **Federal Trade Commission Act** and FTC guidance, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Gramm-Leach-Bliley Act Safeguards Rule for financial institutions, the HIPAA Security Rule for covered entities and business associates, and state security procedures laws, among others. These data security standards and frameworks continue to evolve. In January 2017, NIST proposed updates to its Cybersecurity Framework.
- **State attorney general enforcement.** The enforcement authority of state attorneys general under state privacy and data security laws continues to expand. In 2016, state attorney general regulation of privacy policies and marketing and advertising to state minors increased when the Delaware Online Privacy and Protection Act went into effect. In 2016-2017, the number of state breach notification laws requiring a company to notify state attorneys general about a breach in addition to affected individuals and the number of security procedures laws increased. In 2016, the California Attorney General described a minimum level of information security for companies that collect or maintain personal information should meet regarding

reasonable security. State attorneys general also have enforcement authority under federal privacy and data security laws such as HIPAA and the Children's Online Privacy Protection Act. Whether the influence of state attorneys general in privacy and data security grows stronger with changes at federal regulators of privacy and data security such as the Federal Trade Commission is an area to watch.

- **EU legislative** The EU Data Protection Directive (enacted in 1995, when the internet was in its infancy) will be replaced effective May 25, 2018 with the General Data Protection Regulations (GDPR). While the GDPR updates the EU Data Protection Directive in many respects – including more uniform data protection standards and enforcement – it comes with eye-popping new penalties for non-compliance (up to 4 percent of a company's annual revenues) and extends the EU regulators' jurisdictional reach. Every company doing business with EU residents should get up to speed on the GDPR requirements, and some will be required to appoint EU data protection officers.
- **Canada developments.** On July 1, 2017, a private right of action for persons affected by violation of certain provisions under Canada's Anti-Spam Law (CASL), including anti-spam provisions, will come into effect. Penalties are up to C$200 per breach, to a maximum of C$1,000,0000 per day, plus damages and expenses. Class action lawsuits are anticipated. CASL applies to all commercial electronic messages where a computer system located in Canada is used to send or access the commercial electronic message, subject to certain exceptions. Companies (including U.S. companies) should revisit their compliance with CASL if applicable. In addition, it is anticipated that in 2017 the Canadian government will issue regulations implementing mandatory breach notification to the Canadian Privacy Commissioner, individuals and other organizations and government entities under the Personal Information Protection and Electronic Documents Act (PIPEDA), which is the federal private sector privacy law. Currently, the Alberta private sector privacy law, the Alberta Personal Information Protection Act, requires breach notification to the Alberta Privacy Commissioner, which can direct notification to individuals.
- **Privacy and data security laws around the rest of the world.** The number of countries enacting comprehensive data protection laws keeps expanding. Many of these national laws follow the model of the European Union – sometimes in a transparent bid to be recognized as providing "adequate protection" under EU standards and thus permit the free flow of EU resident data across their borders. Qatar and the Philippines are recent additions to the data protection legislation "club." Such comprehensive data protection laws increasingly are in contrast to those in the United States, with its numerous and various federal and state privacy laws.