O'NEILCANNON
HOLLMAN DEJONG & LAING S.C.

FEDERAL TRADE COMMISSION AND ENFORCEMENT OF PRIVACY LAW

As we have mentioned previously, there is no overarching federal data privacy law in the United States. By contrast, the European Union's General Data Protection Regulation (GDPR) regulates data privacy, including consumer data, in all sectors. Although there is no overarching federal data privacy law in the United States, there are a few sector-specific laws. In health care, for example, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) govern many aspects of privacy. Also, the Telecommunications Act and the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) touch on privacy issues in marketing. Still, there is no federal law specifically regulating the use of consumer data.

Despite the lack of consumer privacy statutes in the United States, the Federal Trade Commission (FTC) has been active for years in protecting American consumers against certain unfair and deceptive practices involving data privacy. The Federal Trade Commission Act (FTC Act) includes an extremely brief section that serves as perhaps the most important provision in U.S. privacy law. Section 5 of the FTC Act states simply: "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." This single line, which does not specifically mention privacy, has been used by the FTC and Congress to make the FTC the de facto privacy enforcement agency of the federal government.

The FTC defines "Unfair Trade Practices" as any practice that results in a substantial injury, that lacks offsetting benefits, and cannot be easily avoided by consumers. In the privacy context, the FTC often looks at practices that unreasonably leave consumers' data vulnerable to hacking or theft. Should a company collect the personal data of an individual in connection with a product or services and make inadequate efforts to protect that data, the FTC may seek enforcement for violation of Section 5 of the FTC Act. Conversely, "Deceptive Trade Practices" involve material statements or omissions that are likely to mislead consumers who are otherwise acting reasonably. Deceptive practices can include false representations or false promises. Importantly, the FTC has taken the position that failure to adhere to the steps, standards, and promises contained in a privacy notice is a deceptive trade practice. Thus, for example, should a company state in its privacy notice that it will not transfer a consumer's data to a third party, any subsequent transfer of data to third parties is likely to be considered a deceptive trade practice.

The financial penalties for unfair or deceptive trade practices can be enormous. These financial penalties can be imposed through a consent decree or through fines imposed by the FTC and approved by the courts. In many instances, the FTC will seek a consent decree with the company through which the company agrees, without admitting guilt, to pay certain fines, stop the alleged practices, or implement new or improved privacy policies and practices. Alternatively, if the company refuses to enter a consent decree, the FTC can seek judgment through an administrative law judge. Should the company refuse to adhere to the FTC ruling, it may be fined up to $43,280 per violation and be liable for any damages caused by the alleged acts. Importantly, each instance of the alleged privacy violation constitutes a unique violation for the purposes of such penalties, leading to potentially substantial fines.

Over the past several years, the FTC has been increasingly active in enforcing unfair and deceptive trade practices that concern consumer data privacy. In 2019 alone, the FTC brought 130 spyware and spam cases as well as 80 general privacy lawsuits. The biggest privacy case of 2019 was *In the Matter of Facebook*, in which the FTC and the social media giant agreed to a consent decree requiring Facebook to pay a five billion dollar fine and institute a broad and privacy-related corporate restructuring. This year, the FTC has commenced 102 actions related to privacy, including cases against Zoom Video Communications, Inc., Williams Sonoma, Inc., and the Western Union Company.

The ability of the FTC to impose substantial penalties on companies who willingly or unwillingly deviate from the practices described in their privacy notices makes it extremely important to routinely review and update your company’s privacy notice to ensure that it accurately depicts your company’s privacy practices.