Recent Data Privacy and Security Representations

Data Privacy Matters

- We are currently defending Google in a high-profile privacy class action filed by Boies Schiller and Susman Godfrey regarding various Google offerings including Chrome, Google Analytics, and Google Ad Manager. The complaint asserts federal and state wiretapping claims, as well as state constitutional and common law privacy claims, on the allegation that Google receives users' communications with websites and personal information when users are browsing the web in "private" or "incognito" mode.

- We represent **IBM** in defending multiple class actions by Illinois residents asserting claims under Illinois's Biometric Information Privacy Act (BIPA). Plaintiffs allege that IBM's "Diversity in Faces" project—in which IBM allegedly conducted facial scans of approximately 1 million photos uploaded to Flickr and made publically available in an online database for the purpose of enhancing diversity in facial recognition technology—violated various notice, consent, and release requirements under BIPA. Plaintiffs seek $5000 statutory damages for each of the 1 million photos that is a photo of an Illinois resident.

- We are defending **IBM Corp**. and its subsidiary, **TWC Product and Technology, LLC**—owner of **The Weather Channel Mobile App**—in a high-profile lawsuit brought by the Los Angeles City Attorney on behalf of the People of California in California state court alleging that TWC's purported failure to disclose its use and sharing of users' geolocation data for advertising and other commercial purposes violates California's Unfair Competition Law ("UCL"). The People seek penalties of up to $2500 for each alleged misuse of user geolocation data, which could amount to billions of dollars.

- We are also defending **IBM** and **TWC** in a putative class action in the U.S. District Court for the Northern District of Florida relating to the **The Weather Channel App's** data privacy practices. The class alleges that IBM and TWC violated Florida's Deceptive and Unfair Trade Practices Act ("FDUPTA"), and also asserts common law claims for fraudulent and negligent misrepresentation/omission and unjust enrichment/restitution.

- We are representing **Google** in the very first class action to be launched in France since the extension of this type of procedure to personal data matters in 2016. Major French consumer association UFC-Que-Choisir filed a claim in June 2019 before the Paris Civil Court and alleged Google breached the European general data protection regulation (GDPR), more specifically its information and consent requirements. The plaintiff is seeking an award of up to EUR 27 billion in damages for an alleged class of French users of terminals equipped with an Android operating system and a Google account.

- We are advising **numerous multinational corporations** on compliance with GDPR in their collection and processing of EU-based personal data, as well as in the production of that data in U.S. and non-EU litigation proceedings.

- We obtained summary judgment in California state court for **a major wireless telecommunications company** arising out of alleged disclosure of confidential consumer information. The matter involved allegations of negligence and breach of privacy arising from allegedly divulging private consumer information to third parties. The decision was upheld by the California Court of Appeal.

- We represent **a large financial services company** in an SEC investigation into potential violations of privacy-related securities rules and related disclosure issues.

- We represented **comScore, Inc.**, in a data privacy class action in the Northern District of Illinois. The plaintiffs asserted that comScore, a company that measures consumers' online behavior, obtained information about their Internet usage and other personal information without adequate consent.

- One of our partners successfully defended **Hulu** against consolidated putative class action cases involving the Video Privacy Protection Act and related privacy statutes, and the allegation that the defendant knowingly disclosed personally identifiable information about its users. Defeated class certification and obtained summary judgment on liability.

- One of our partners successfully defended **Take-Two Interactive**, publisher of the NBA 2K basketball video games, against a class action alleging violation of the Biometric Information Privacy Act ("BIPA") based on use of user photographs to create customized game players and transmit them to third party users when playing in multiplayer mode. The decision was affirmed on appeal.

- One of our attorneys defended **VIZIO** in an investigation by the US Federal Trade Commission (FTC) concerning VIZIO's data collection and use practices. The FTC alleged that VIZIO engaged in unfair trade practices that violated the FTC Act and that VIZIO failed to adequately disclose the nature of its "Smart Interactivity" feature and misled consumers with its generic name and description. The precedent-setting enforcement action ended in the FTC establishing a new industry standard for data collection from Smart TVs and VIZIO agreeing to bolster its disclosure practices. VIZIO neither admitted nor denied the allegations.

- For **a government client**, we have advised on implementing a suite of data privacy and information security regulations across a truly diverse facility base. For the same client, we are assessing what new procedures/protections should be put into place to avoid future data breaches.

- We are intervening for **Lycos, Inc.** and **Wired News** in a case brought by the Electronic Frontier Foundation against AT&T for giving the NSA access to its fiber-optic telecommunications system. EFF's claims involve breach of privacy allegations; they have filed multiple documents under seal that were given to them by a former AT&T employee. Wired

News has obtained and published some of the sealed documents and is seeking to unseal the rest of them.

- We were involved in a series of high-profile investigations by the U.S. and other governments into marketing practices and payments made to **healthcare providers**, including products such as Trileptal and TOBI, but also allegations on antitrust, data privacy, and other compliance-related issues in many jurisdictions. We set up a system ensuring compliance with relevant data privacy laws in the respective jurisdiction; in addition, we assisted in setting up a mechanism through which relevant personal data could be shared between the U.S. and Europe.

- We won dismissal of a SDNY case against our client **Harley-Davidson**. The claims arose from loss of a computer with personal information of Harley-Davidson motorcycle owners.

- We won summary judgment for **Home Depot** in a class action in the Southern District of California alleging violation of a credit card privacy statute.

- One of our partners represented the German company **Merz Pharmaceuticals** in a U.S. pharmaceutical litigation concerning its Alzheimer's disease treatment Namenda®. Document discovery in that case implicated both the German Data Protection Act as well as HIPAA in the U.S. To comply with the law, all documents containing patient and personal employee data were hosted and reviewed in the EU with protected data being redacted before the documents could be brought into the U.S. for production.

- One of our attorneys advised **an internet content provider** on consumer privacy policies.

- One of our attorneys advised **an international confectionery manufacturer** with regard to compliance related data privacy issues in the context of internal investigations (including on limitations to access/search German employees' e-mail accounts).

- We represented **DIRECTV** in a class action matter alleging violations of the Electronic Communications Privacy Act ("ECPA"). We obtained a decision from the Ninth Circuit Court of Appeal affirming the dismissal of the complaint. In a case of first impression, the Court concluded that the ECPA did not permit liability for aiding and abetting or conspiracy to violate Section 2702 of the Act.

- We obtained a $2.3 million judgment after a unanimous jury verdict finding 103 violations of the DMCA, Electronic Communications Privacy Act, and Federal Communications Act arising from defendant's distribution of illegal signal theft devices designed to steal **DIRECTV**'s satellite programming.

Cyber Security Matters

- We are representing a **large mortgage lending/financial services company** in connection with a potential vulnerability in a database containing millions of records of personal identifying information.

- We are overseeing investigation of a potential data breach for a **large financial industry company** including determining whether the incident resulted in any personally identifiable information being made available outside the company, and whether any notice obligations were triggered under the data security laws of any of the 50 states.

- We represent the **former CEO of Equifax**, **Rick Smith**, in connection with one of the most significant data breaches in recent history. The breach involved the theft of personal data of more than 145 million people in the U.S., Canada, and the United Kingdom. We worked with the company, outside consultants, and our client to quickly understand the size and scope of the breach and the resulting investigation into the cause, in order to prepare Mr. Smith to testify before multiple hostile congressional committees. We also currently represent Mr. Smith in multiple lawsuits asserting claims arising from the data breach.

- We have advised **numerous industry leaders** on preparing for or responding to a breach incident.

- We are representing **one of the world's largest banks** in connection with a highly publicized data breach caused by a rogue employee. Within days of the breach, we worked directly with the client to conduct a thorough investigation into the cause and extent of the data breach. We also assisted the client with devising a strategy to address customer concerns. Simultaneously, we managed the bank's responses to both federal and state regulators (including the SEC Compliance Branch, the SEC Enforcement Branch, the FBI, the FTC, the CFTC, the FDIC, FINRA, the Federal Reserve, and numerous state regulators from across the United States) and foreign financial regulators (from Australia, Singapore, Japan, and all across Europe). We ensured that all regulatory responses were consistent and complete, minimizing the potential for formal investigations.

- We advised a **South Korean company with global operations** regarding its notification obligations under the data protection regulations of over 100 different countries following a data security breach. We also represented the company in responding to a Civil Investigative Demand (CID) from the U.S. Federal Trade Commission and inquiries from the U.S. Senate, the UK Information Commissioner's Office, and German authorities.

- We advised a **leading U.S. computer company** in a matter involving leakage of highly confidential information (including information about the client's new products and marketing strategy) through the hacking of an email account of the client's partner in Russia. The complications included suspicions that the information was passed to the client's European competitor. We handled internal investigation into activities of the client's Russian partner as well as its former and current employees, interviews with the suspects, criminal investigations in Russia and Europe, and cooperation with the outside U.S. forensic experts.

- We obtained a complete victory for **IBM**, who had been named as a defendant in a series of state and federal class actions arising out of the loss of nine data tapes belong to IBM's client, Health Net, Inc. Plaintiffs sought $2 billion in alleged damages. After the cases were consolidated in the Eastern District of California, Quinn Emanuel filed a motion to dismiss on standing grounds, which the Court granted. During the months that the motion was pending, Quinn Emanuel also managed to stave off discovery by demonstrating to the Judge that they had a robust motion to dismiss and that causing IBM to engage in discovery before the motion was decided would be a miscarriage of justice.

- We represent the **audit committee** of a board of directors of a public company in conducting an independent inquiry into the company's cybersecurity maturity following a "noisy" resignation by the company's CISO.

- We advised **a large international insurer** on possible legal implications arising from the use of data from its claims and underwriting files.

- We successfully represented data aggregator **Choicepoint** in numerous data privacy theft cases and obtained dismissal of all claims.

- In a highly confidential matter, we represent **a multinational corporation** with respect to illegal hacking into their computer systems.

- We advised **a major hospitality company** regarding regulatory and other potential claims regarding a data breach.

- We represent **a major entertainment industry client** with respect to the issues arising from the well-publicized hack of Sony Corporation.

- We are overseeing a data breach matter for **a multinational entertainment company** including 50 state law compliance with notification rules, counseling reactions against the hacker(s), potential class action cases, notification to litigants and courts where documents subject to "lit hold" notices are compromised, etc.