Data Privacy and Security

Consumers and regulators are more focused than ever on companies' data privacy and security practices. There has been a surge in government investigations, enforcement actions, and class action lawsuits challenging those practices under existing laws, and that surge will continue with the passage of new laws, such as California's Privacy Rights Act (CPRA), Illinois's Biometric Information Privacy Act (BIPA), and similar biometric information privacy laws adopted in Texas, Washington, and New York City and being considered in other jurisdictions. These laws regulate what personal and biometric information companies can maintain and how it can be gathered, stored, and protected.

We represent some of the world's largest companies—in a broad array of industries including technology, mobile app development, digital advertising, telecommunications, finance, healthcare, media and insurance—in investigations and lawsuits challenging the collection, use, storage, and/or dissemination of customer and user data. Our Data Privacy and Security litigators' in-depth understanding of this fast-changing area of the law, combined with Quinn Emanuel's unrivaled litigation prowess and global scope, makes us uniquely positioned to handle these matters. Clients hire us to handle their most difficult and cutting edge Data Privacy and Security cases when substantial penalties or damages are on the line.

We also advise clients seeking to use their data to enhance the customer experience and develop new business opportunities minimize litigation risk and maintain compliance with recently-enacted privacy legislation, such as the CPRA and biometric information privacy laws.

Our Data Privacy and Security lawyers include former government officials who bring a unique perspective to these cases, particularly when dealing with state and federal agencies. One of our partners, for example, recently served as the Executive Deputy Attorney General of the Economic Justice Division in the New York Attorney General's office and supervised every data privacy and security investigation and enforcement action for New York State. Another of our partners recently served as Deputy Chief of Staff of the SEC, where he was responsible for assisting the SEC Chair in developing the agency's policies on cybersecurity disclosure and data protection for registered entities and public companies, and was involved in both inter-agency and public-private efforts to plan for and coordinate responses to cybersecurity events.

Our Data Privacy and Security lawyers are located in the United States, Europe, Asia and Australia, and we regularly coordinate in order to stay abreast of data privacy and security laws that affect our international clients in multiple jurisdictions.

With respect to Data Security in particular, we have successfully represented numerous companies faced with data security breaches. We understand that threats to your cyber security can create significant operational and legal problems. They require an aggressive, fast-paced, multi-disciplinary plan to control and even prevent potential damage. Quinn Emanuel can work with you to design such a plan—one you

can activate immediately in the event of a breach. We can work with you to update your current strategy or rapidly design and implement an entirely new plan if you do not already have one in place.

We can quickly activate an experienced team that will address all aspects of the matter that are likely to arise, including regulatory, state, and federal government investigations, class actions, and public relations. We have nationally recognized experts in each of these fields who can help your company navigate the thicket of issues that accompany a data security incident. We have nine offices in the U.S. and thirteen more located in Europe, Asia, and Australia. Thus, we have the resources in place, poised to act on a moment's notice, no matter when or where the incident occurs.

As soon as a security breach becomes public or customers receive notice, multiple class actions are filed and continue to be filed over the succeeding weeks and even months. These suits are now commonly filed within hours of an event being public. Such suits are faring better in courts. In addition, a wide array of regulators commence their own investigations. Quinn Emanuel's experience with these cases, and its preceding reputation as a litigation powerhouse, gives our clients an edge in disposing of these cases as quickly as possible.

Almost no company is free of risk. Any company that stores private consumer or employee information can be a target of a security breach. Preventive care is important, both for corporate diligence and board and management peace of mind. We offer a **Readiness Audit**, which will assess the strength of your company's data security, its preparedness in the event of an attack, and help to design a plan to bolster areas that are not sufficiently robust.

REPRESENTATIVE MATTERS

DATA PRIVACY MATTERS

- We defended **Google** in a high-profile privacy class action 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 defeated the damages class, which sought billions in damages. Shortly before trial, we favorably settled the certified injunctive relief class by mainly amending some disclosures and no money flowing to the class.

- We represented **Kaseya**, a computer-software company, in a case brought by a customer after Kaseya was the victim of a ransomware attack. Despite clear contractual language prohibiting the suit, Plaintiff chose to sue anyway. Kaseya moved to dismiss the Complaint, and the Court adopted all of Kaseya's arguments as to why the case should be dismissed and dismissed Plaintiff's complaint in its entirety.

- Currently defending **Match Group, Inc. and its affiliated dating sites** (e.g. Tinder, Match.com, OKCupid, Plenty of Fish) against a mass arbitration campaign launched by Labaton Sucharow. The Claimants allege that the Dating Sites use facial recognition technology in violation of Illinois' Biometric Information Privacy Act.

- Currently defending **Match Group, Inc. and its affiliated dating sites** (e.g., Tinder, Match.com, OKCupid, Plenty of Fish) against a putative class of Illinois residents who claim that the Dating Sites scanned their profile photos with facial recognition technology without consent and in violation of Illinois' Biometric Information Privacy Act.

- Currently defending **Match Group, Inc., Match Group LLC, and Tinder** against a putative class of Illinois residents who claim that Tinder's selfie- and video-verification features fail to comply with Illinois' Biometric Information Privacy Act.

- We represented **Ancestry.com** in a putative class action filed in the Northern District of California. Plaintiffs allege Ancestry violated their rights to publicity by using personal information from plaintiffs' (and millions of others') yearbooks to advertise Ancestry's paid services. Plaintiffs assert class claims under California's right of publicity statute; for common law "intrusion upon seclusion"; and based on various other derivative, state law theories. We were able to convince the court to dismiss all of plaintiffs' claims. The court first determined that although Ancestry may have profited from use of plaintiffs' information, that was not enough to establish a "concrete injury" for purposes of Article III. The court also ruled that although Ancestry uploaded the information to the internet and reformatted it, this conduct fell within the traditional role of a "publisher," and Ancestry is thus entitled to immunity under section 230 of the Communications Decency Act.

- Currently defending **Google** in *Calhoun et al. v. Google LLC*, a high-profile data privacy class action in which the plaintiffs seek to recover billions of dollars on behalf of all U.S.-resident Chrome users on the basis of Google's alleged misappropriation of Chrome users' personal data through its third-party web services such as Ad Manager, Analytics, Embedded Maps, Fonts, and other services. The complaint asserts sixteen causes of action, including federal and state wiretapping claims, breach of contract, unfair competition, and state law constitutional and common law privacy claims.

- We represent **IBM** in defending multiple class actions by Illinois residents asserting claims under 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.

- One of our partners successfully defended **Take-Two Interactive**, publisher of the NBA 2K basketball video games, against a class action alleging violation of Illinois' 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.

- We successfully defeated an Illinois BIPA class action on behalf of an international manufacturer with plants located throughout Illinois. We obtained a settlement after we identified and pursued a defense that posed an existential threat to the plaintiffs' claims. We successfully leveraged this defense in a way that allowed our client—who was going through

restructuring—to efficiently resolve the case for an amount well-below the market rate for a BIPA settlement at the time.

- We recently obtained a significant victory for **hiQ Labs, Inc**. over LinkedIn Corporation in the U.S. Court of Appeals for the Ninth Circuit, which held in precedential opinion that scraping data from a public website does not violate the Computer Fraud and Abuse Act ("CFAA"). The Ninth Circuit held that the statute's prohibition on accessing a computer network "without authorization" does not extend to public websites. This holding represents a significant win for the open internet, and prevents website operators from invoking the federal computer hacking statute to enforce their terms of service against users who access only data that is not password-protected.

- Successfully defended **IBM** and its subsidiary, **TWC Product and Technology ("TWC")—** 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 violated California's Unfair Competition Law. Following TWC's filing of motions for summary judgment, the City Attorney agreed to dismiss its claims with no penalty or admission of wrongdoing by TWC

- Successfully defended **IBM** and **TWC** against a putative class action in the U.S. District Court for the Northern District of Florida relating to The Weather Channel App's data privacy practices. Plaintiffs asserted claims for violation of Florida's Deceptive and Unfair Trade Practices Act, fraud, negligent misrepresentation, and unjust enrichment. The court dismissed several claims on TWC's motions to dismiss and the remaining claims before class certification.

- Defending **TWC** in a putative class action in the U.S. District Court for the Northern District of California relating to The Weather Channel App's data privacy practices. Plaintiffs allege that TWC's use of geolocation data for advertising violated users' right to privacy under the California Constitution, resulted in unfair competition, and that TWC was unjustly enriched.

- 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 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 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 intervened on behalf of **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 involved breach of privacy allegations; they filed multiple documents under seal that were given to them by a former AT&T employee. Wired News obtained and published some of the sealed documents and sought to unseal others. We successfully obtained an order unsealing many of the documents Wired News sought.

- 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 advised a **leading U.S. technology company** in a cyber incident response relating to ransomware that targeted source code. We coordinated negotiations with the ransomware threat actor, and directed the internal investigation, including interviews of vendor employees in India and direction of experts inside and outside the United States. We also coordinated law enforcement reporting.

- 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 represented **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.