PUBLICATIONS | 12.13.2022

2022 BBA Privacy & Cybersecurity Conference Takeaways

Choate sponsored the Boston Bar Association's 2022 Privacy & Cybersecurity Conference. After two years in the virtual format, the annual conference returned in-person at the Boston Bar Association on December 8th. Attendees heard from top privacy, cybersecurity and digital law practitioners and industry experts on the latest trends and cybersecurity topics.

Below are key takeaways from the conference.

The Prosecution of Uber's Former Chief Security Officer: Broader Lessons

In October 2022, Uber's former Chief Security Officer was convicted of obstruction of justice because of actions he took while the Federal Trade Commission (FTC) was investigating a data breach at Uber. During the course of the investigation, Uber suffered another similar data breach that its Chief Security Officer did not disclose to the FTC or Uber's attorneys, who were interfacing with the FTC. Instead, the Chief Security Officer modified Uber's "bug-bounty" program—a routine program organizations use to compensate so-called "white hat" hackers who report software bugs. The CSO used this program to pay $100,000 to the hackers who caused the second data breach in exchange for the hackers agreeing to destroy the data they stole and providing an affidavit falsely stating that they did not steal any data.

While many of the facts underlying this criminal prosecution are unique, there are larger takeaways for organizations and their employees when responding to data breaches, including:

- If you are engaged in conversations with government enforcement agencies regarding cybersecurity incidents, you must be fully forthcoming and not selectively disclose information.
- Companies must ensure that any factual representations made to the government are accurate.
- Hackers' promises to destroy and not disclose stolen data do not relieve victim companies of data breach reporting obligations.

The Current Threat Environment's Impact on Cyber Insurance

In recent years, the size of the cyber insurance market has skyrocketed, but with the surge in demand for coverage comes increased data on claims and premiums—allowing insurers to better underwrite their products.

In January 2022, Merck & Co. had a $1.4 billion victory in New Jersey litigation against insurers over losses from NotPetya malware. As a result of the Merck decision, insurers are better defining their "war exclusions" so that policies do not provide coverage for cyber-attacks that are attributed to state actors. Attributing an attack to a state actor is incredibly difficult, though, and likely a source of future litigation. It seems doubtful that a federal backstop for catastrophic cyber events will occur given the polarization in Congress.

Change is the Only Constant: Developments in State Privacy Laws in 2023

State-level momentum for comprehensive data privacy laws continues, as it seems unlikely that Congress will pass a comprehensive federal law anytime soon. Five states (California, Colorado, Connecticut, Utah, and Virginia) have enacted

comprehensive data privacy laws. California's Consumer Privacy Act (CCPA) went into effect in January 2020, while the other four state laws, along with California's Consumer Privacy Rights Act (CPRA), are set to become effective in 2023.

This year brought the first CCPA enforcement action with California announcing a $1.2 million settlement with Sephora, underscoring the need for companies to ensure they are compliant with all relevant state laws and heed agency enforcement guidance. Companies should review and update internal and public-facing policies, and regularly review relevant protocols to ensure requirements are fulfilled (e.g., ensure that the ability for consumers to opt-out of the sale of personal information functions appropriately).

Weaponizing Surveillance: Post-Dobbs Uses of Surveillance Technologies and Their Impacts on Marginalized Communities

The repeal of Roe v. Wade in the Supreme Court's recent Dobbs decision set off a wave of state laws criminalizing abortions under certain circumstances. These laws give rise to concerns that customers' and patients' digital information, such as text messages, search queries, location data, and reproductive health data, are now being collected as evidence of criminal intent. What should health organizations do?

- Align your boards and trustees on your mission statement. Any policies you adopt and stances you take will come under intense political, legal, and media scrutiny; be ready with a unified front.
- Inform customers about data protection options. The consequences for unwanted transmission of reproductive health information—and adjacent data—have gotten murkier. What do patients need to know from you in order to be able to make proactive requests to protect information?
- Anticipate data protection issues. Understand that your policies on data sharing and cooperation with government investigations may be critical to customer/patient wellbeing.

Printable version.

Adam J. Bookbinder
Co-Head of Government Enforcement & Compliance

Elizabeth Powers
Of Counsel