KEKER
VAN NEST
& PETERS

Navigating the Privacy Minefield: Regulatory and Litigation Trends & Case Studies

March 27, 2025

Presenters

Andrew Dawson
adawson@keker.com

Puja Parikh
pparikh@keker.com

Melissa Cornell
mcornell@keker.com

Agenda

- The Privacy Landscape
  - Common causes of action
  - Recent litigation trends
- The Regulatory Environment
  - The past few years: rise of states, congressional legislation, executive action
  - Expectations under the Trump Administration
- A Case Study: *United States v. Sullivan* and *Solar Winds*
  - Lessons to learn (mistakes were made)

The Privacy Landscape

Privacy law is a patchwork.

- **Common law invasions of privacy**
  - Intrusion upon seclusion, misappropriation of name or likeness
- **Consumer remedies**
  - Unfair Competition Law, California Consumer Legal Remedies Act, fraud, breach of Contract, unjust enrichment
- **State statutes**
  - California Invasion of Privacy Act (CIPA), California Consumer Privacy Act (CCPA)
- **Federal statutes**
  - Wiretap Act
  - Stored Communications Act
  - Computer Fraud and Abuse Act

In the last decade, we have seen a wave of state privacy statutes.

- In the absence of a federal statutory regime, states have embarked on filling the gap in privacy law with their own laws.
- Over 40 percent of states have implemented consumer privacy laws, starting with the California Consumer Privacy Act (CCPA).
- States are now turning their focus to other areas, like consumer health data and children's privacy.
- These state laws are often backed by bipartisan support.
- In 2024, we saw a surge in states passing new privacy laws that are either now in effect or will be going into effect through 2026.

Proposals for a federal privacy bill exist, but momentum has stalled under the new administration.

Innovation, Data, and Commerce Subcommittee Hearing: "Promoting U.S. innovation and Individual Liberty through a National Standard for Data Privacy" (March 1, 2023)

Cathy McMorris Rodgers (R-WA), House Energy and Commerce Committee Chair

"Americans have no say over whether and where their personal data is sold and shared, they have no guaranteed way to access, delete, or correct their data, and they have no ability to stop the unchecked collection of their sensitive personal information."

"This isn't acceptable. Data brokers and Big Tech's days of operating in the dark should be over."

"People should trust their data is being protected."

Proposed “American Privacy Rights Act of 2024” – H.R. 8818

- Bipartisan and bicameral draft legislation introduced on June 25, 2024 by Congresswoman Cathy McMorris Rodgers (R-WA) and referred to the House Committee on Energy and Commerce
- Aims to establish a national privacy standard at the federal level
- Provides a private right of action for violations of data privacy rights under the proposed Act; also enforceable by the FTC and State attorneys general
- Prevents companies from enforcing mandatory arbitration in cases of substantial privacy harm
- Expressly sets “data minimization” limitations on how companies can use consumer data

Spotlight: California Consumer Privacy Act of 2018

The CCPA is a first-of-its-kind consumer privacy law, passed in 2018 and effective as of 2020

- The most comprehensive data privacy law in the United States

Passed just one month after the European Union's General Data Protection Regulation (GDPR)

- Both laws impose civil fines for misuses of consumer data

Aimed at providing the California Attorney General broad enforcement powers, with limited private right of action for breaches of unecrypted personal information

Spotlight: California Consumer Privacy Act of 2018

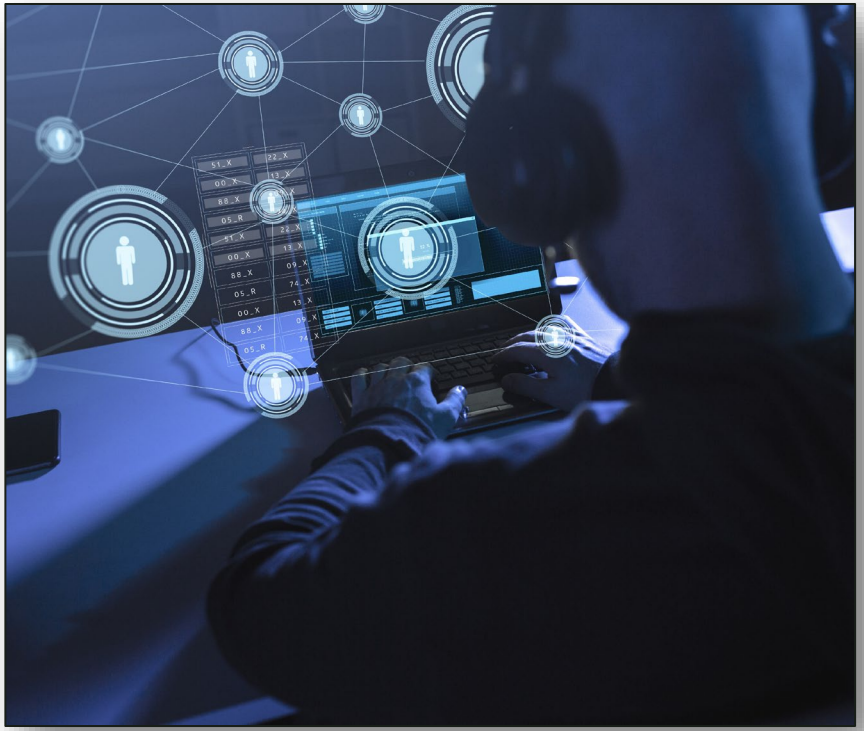
GDPR

- “Rights” model
- Principle-based approach
- Informed, opt-in consent
- Right to be forgotten

CCPA

- “Protection” model
- Deception and unfairness
- Opt-out
- Right to delete

Spotlight: California Consumer Privacy Act of 2018



Consumer rights under the CCPA

- Right to know
- Right to delete
- Right to opt-out of sale or sharing
- Right to correct
- Right to limit use and disclosure of sensitive personal information
- Right to non-discrimination

Spotlight: California Consumer Privacy Act of 2018

CCPA applies to

- For-profit businesses in California, *and*

- Gross revenue of over $25 million, or
- Buy, sell, or share the PI of at least 100,000 California residents or households, or
- Derive 50% or more annual revenue from selling PI

Spotlight: California Consumer Privacy Act of 2018

***People of the State of California v. Sephora USA, Inc.*, 2022 WL 22913962 (Cal. Super. Ct. August 24, 2022)**

- Investigation into the privacy practices of Sephora for its collection, use, and sale of consumers' online activities and other personal information
- Allegations
  - Violations under the CCPA and UCL
  - Sephora, like many online retailers, installed tracking software enabling third parties to surveille and monitor consumers as they shop, collecting information like purchasing information and even location
- Settlement
  - Compliance program, assessment, and reporting requirements
  - $1.2 million in fines

Big Data in the Crosshairs

- **Increased litigation targeting not only how data is collected, but also how data is *stored* and *used***
- **Examples:**
  - Location information
  - Browsing activity
  - Purchase history
  - “Cookie” tracking
  - App-usage data
  - Biometric data
  - AI privacy suits

Notable Recent Class Action Settlements

In re: Facebook, Inc. Consumer Privacy User Profile Litigation (N.D. Cal.) - $725M

- Allegations of granting third parties access to user content and PI without consent

In re: T-Mobile Customer Data Security Breach Litigation (W.D. Mo.) - $350M

- Allegations of failure to adequately protect consumers' PII from data breach

In re. Capital One Consumer Data Security Breach Litigation (E.D. Va.) - $190M

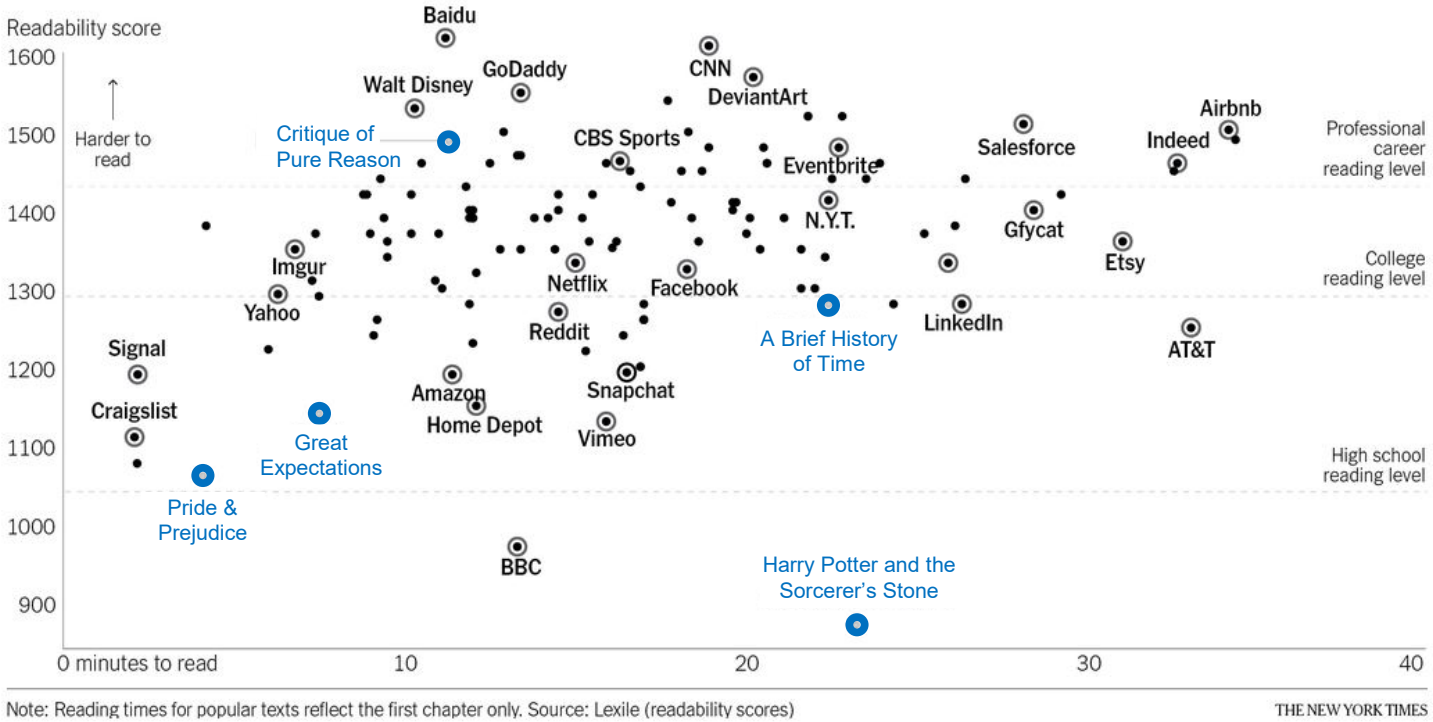
- Allegations of failure to adequately protect consumers' PI from data breach

Terms of Service & Privacy Policies

Front line of defense

- **Relevant to consent and disclosure-based defenses**
- **Disclosures can be used to defeat elements of common claims (*e.g.*, expectation of privacy, reliance) at the pleadings stage and at class certification**
  - *E.g.*, *In re Google Inc. Gmail Litig.*, No. 13-MD-02430-LHK, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014) (declining to certify class alleging Wiretap Act violations because of the "panoply of sources from which email users could have learned of," and thus impliedly consented to, the alleged interceptions)
- **Broad and clear disclosures in plain English are the most defensible**
- **Online contract formation**

Terms of Service & Privacy Policies



"We Read 150 Privacy Policies. They Were an Incomprehensible Disaster."

--Kevin Litman-Navarro, *The New York Times*

Preparing for a Data Breach – Not a matter of If, but When

- **Understanding compliance obligations**
- **Understanding how data is collected, stored, used**
- **Understanding the different state laws implicated**
- **Creating an Incident Response Plan**
- **Being prepared for the first 72 hours**

The Regulatory Environment

Privacy Regulatory Environment: The Rise of States

States led the charge in defining and regulating cybersecurity and privacy

- **2024**: Seven states enacted new robust privacy laws, four states' privacy laws took effect
- **2025-26**: Eleven new comprehensive privacy laws will go into effect across various states
- **By 2026**, half the US population will be covered by a comprehensive state privacy law

Across states, these are generally similar laws (ex: Children's Online Privacy Protection Act scope), with few notable differences

Privacy Regulatory Environment: California

- **The California Privacy Protection Agency** – CPPA 2024 initiatives
  - Began privacy enforcement in California
  - Published first two California Consumer Privacy Act enforcement advisories:
    1. Addressing application of data minimization to consumer requests
    2. Addressing avoidance of dark patterns
  - Issued confidential notices of violations to various companies
  - Private right of action may be expansive given court decisions giving broad deference to what constitutes a "data breach"
- **California Attorney General** – still enforcing the CCPA as well
  - Ex: settlement with mobile game company that failed to obtain parental consent for collecting and sharing children's data from a mobile app
- **Protecting Our Kids from Social Media Addiction Act** – nixed

Privacy Regulatory Environment: Congressional Legislation and Executive Action

- **2023**: Biden Administration released National Cybersecurity Strategy

- **2024**: Protecting Americans' Data from Foreign Adversaries Act passes and is signed into law
  - Regulates the transfer of personal data from the US due to national security concerns

- **2025**: Biden issues executive order
  - Provides the federal government more power to sanction hackers and identity theft crimes
  - Largescale implications for federal contractors, particular cloud service and other technology providers

Privacy Regulatory Environment: Agencies

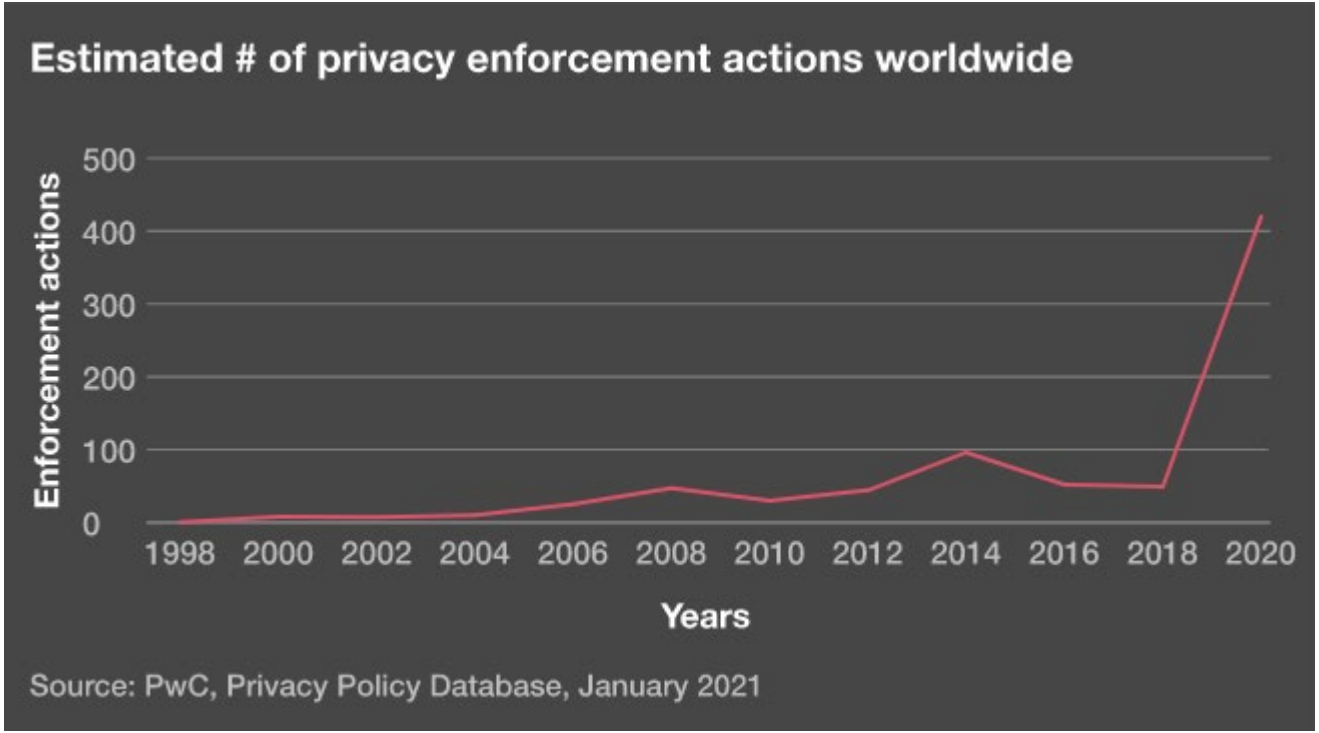
Federal Trade Commission

- Algorithmic bias concern; targeted AI facial recognition technology
- Enforcement of data privacy and use of sensitive consumer information
- Children's Online Privacy Protection Act

Securities and Exchange Commission

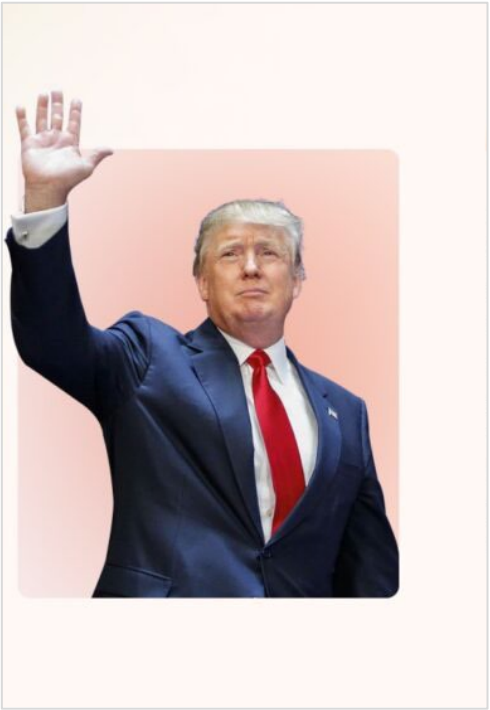
- 2024 was the first full year of new cybersecurity disclosure rules for public companies, requiring disclosure of material cyber incidents
- Historic levels of enforcement activity continued in 2024

U.S. Regulatory Trend: Increasing Enforcement



Source: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/seven-privacy-megatrends/rise-privacy-enforcement.html

Enter the Trump Administration



Cyber is a whole thing. It's a whole new field. We have some tremendous people. We're better at cyber than anybody else in the world. But we weren't really using that power, that intellect, on cyber. We weren't doing it. And now we are. And we have – I have – incredible people in charge of cyber. If we ever get hit, we'll hit very hard. We'll be able to hit very hard. But it's a new form of war – warfare – and I think we have it very well under control.

U.S. Privacy Regulatory Environment: The Trump Era

Securities & Exchange Commission

- Creation of Cyber and Emerging Technologies Unit (CETU)
- Cybersecurity continues to be an enforcement priority, but contours unknown
- Announced focus on “fraudulent” cybersecurity disclosures potentially marks a shift away from SEC cybersecurity disclosure cases to date

Consumer Financial Protection Bureau

- Trump imposes significant operational changes that raise questions about the agency’s future scope and direction
  - Freeze of virtually all CFPB activities by ordering employees to stop all enforcement and litigation activity, halting rulemakings and suspending effective dates of pending rules
  - DOGE has expressed a desire to eliminate the CFPB

U.S. Privacy Regulatory Environment: The Trump Era

Executive Orders

- State and local governments should play a larger role in protecting water utilities, ports, and other critical infrastructure from cyberattacks
- Federal government funding cuts

Case Studies

USA v. Sullivan Overview

- Joseph Sullivan, who served as the Chief Security Officer for Uber from 2015 to 2017.
- Uber experienced a data breach that Sullivan attempted to cover up. Uber was under investigation by the Federal Trade Commission for a similar data breach two years earlier.
- Sullivan was found guilty of obstruction of justice and misprision of a felony for his role.
- Sullivan was sentenced to serve a three-year term of probation and ordered to pay a fine of $50,000.

Case Background: The Uber Data Breaches

Breach
A hacker discovered an AWS key on GitHub, accessing sensitive information of tens of thousands of Uber drivers. This prompted an FTC investigation into Uber's data security practices.

Second Breach
Hackers gained access to Uber's GitHub account, found AWS keys, and downloaded unencrypted data of 600,000 individuals—similar to the 2014 breach but larger in scale. FTC not informed.

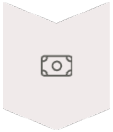
Sullivan Hired
Joseph Sullivan joined Uber as Chief Security Officer and later became Deputy General Counsel. He became heavily involved in Uber's response to the ongoing FTC investigation.

Cover-Up Exposed
New CEO Dara Khosrowshahi discovered the truth about the breach, fired Sullivan, and publicly disclosed the incident. Federal charges followed.

The Cover-Up Strategy

Track Down Hackers
Sullivan and his team identified the hackers who had accessed Uber's systems and downloaded sensitive data of 600,000 individuals.

Non-Disclosure Agreement
They pressured hackers to sign an NDA that *recharacterized* the hack as "research" into "vulnerabilities" under Uber's Bug Bounty Program.



Payment
Uber paid the hackers $100,000 in exchange for their signatures and agreement to delete the downloaded data.

Concealment
Sullivan did not inform Uber's general counsel or the FTC about the breach, and later misrepresented details to the new CEO.

Legal Issues: Obstruction of Justice

Section 1505 provides that "[w]hoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States . . . [s]hall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in [S]ection 2331), imprisoned not more than 8 years, or both."

18 U.S.C. § 1505.

Legal Issues: Misprision of a Felony

Misprision is the crime of "having knowledge of the actual commission of a felony" and "conceal[ing]" or failing to "as soon as possible make known the same to some judge or other person in civil or military authority under the United States."

18 U.S.C. § 4.

To establish misprision, the government is obliged to show that "the principal committed and completed the felony alleged." *United States v. Ciambrone*, 750 F.2d 1416, 1417 (9th Cir. 1984). Here, that meant proving that the hackers had "intentionally accesse[d]" Uber's computers "without authorization . . . and thereby obtain[ed]" information from those "protected computer[s]," in violation of the CFAA.

18 U.S.C. § 1030(a)(2).

Ninth Circuit Affirms Conviction

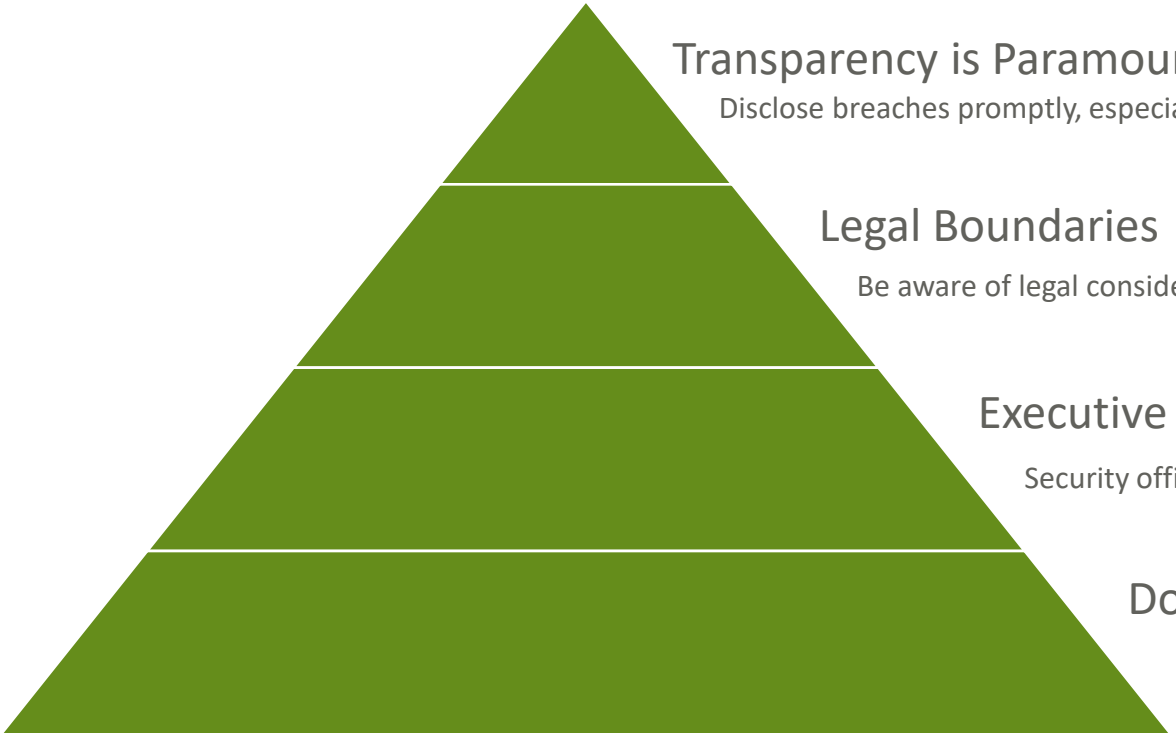
Obstruction of Justice

- No additional nexus required between Sullivan's conduct and the FTC investigation for an obstruction of justice conviction; preexisting elements were sufficient.
- No requirement that Sullivan was under a duty to disclose the information to the FTC for an obstruction of justice conviction.

Misprision of a Felony

- The court rejected Sullivan's argument that the NDA retroactively authorized the hackers' access. Authorization under CFAA is assessed at the moment of access, not after the fact.
- Sullivan, a former prosecutor in a "Computer Hacking and IP Unit," had sufficient knowledge that the conduct constituted a felony punishable by more than a year in prison.

Implications for Cybersecurity Professionals



Transparency is Paramount

Disclose breaches promptly, especially during investigations

Legal Boundaries

Be aware of legal considerations when engaging hackers

Executive Accountability

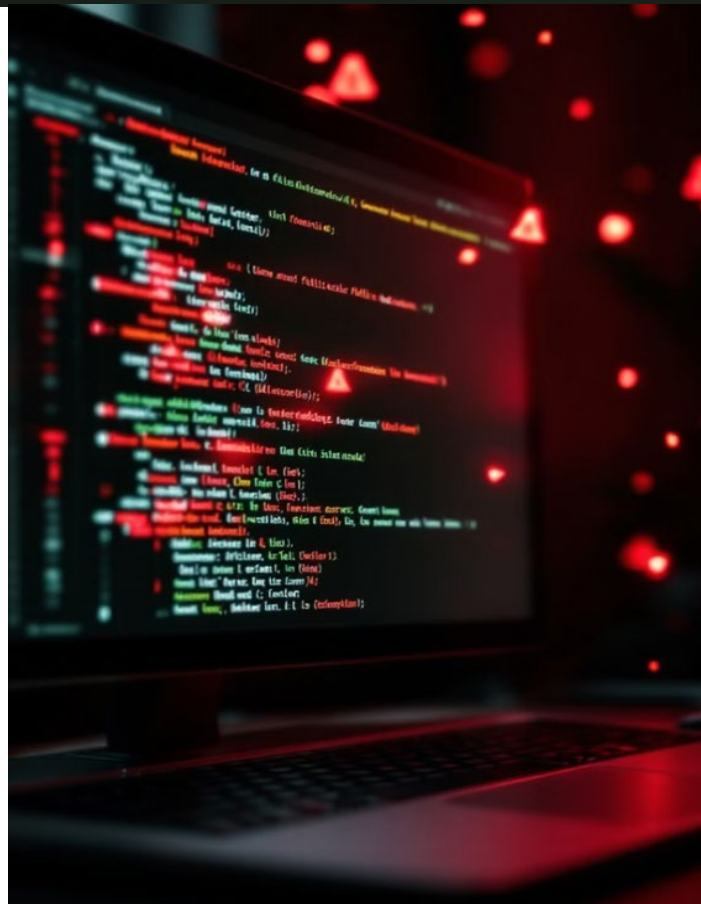
Security officers face personal legal liability for cover-ups

Documentation Integrity

Accurate record-keeping is essential during security incidents

SEC v. SolarWinds Overview

- On October 30, 2023, the SEC filed a complaint against SolarWinds and its Chief Information Security Officer (“CISO”), alleging securities fraud and failures of reporting, internal control over financial reporting, and disclosure controls and procedures, in connection with a compromise of the company’s software product that was publicly revealed in December 2020.
- The complaint filed in SDNY alleges that SolarWinds and its CISO misled investors and customers about cybersecurity weaknesses that enabled a Russian government espionage campaign against U.S. networks.
- This marks the first case where the SEC has charged a CISO individually for cybersecurity violations and the first instance of scienter-based securities fraud charges related to a breach.



Case Background

Company Profile

SolarWinds is a Texas-based company producing software for IT management, with its flagship product Orion used throughout the U.S. by governmental and private entities.

Security Compromise

On December 14, 2020, SolarWinds disclosed that threat actors had inserted a vulnerability into certain versions of Orion, later attributed to the Russian Foreign Intelligence Service.

SEC Allegations

In October 2023, the SEC filed a complaint against SolarWinds and its CISO alleging that they made false and misleading statements and omissions on SolarWinds' website and in its blog posts, press releases, initial registration statement ("Form S-1"), and quarterly and annual SEC reports before the incident, as well as in two current reports on Form 8-K in which SolarWinds disclosed the compromise.

Legal Issues: Fraud and False and Misleading Statements

Website “Security Statement”	Press Releases & Blog Posts	SEC Filings	Form 8-K Disclosures
The court allowed fraud claims related to SolarWinds’ website Security Statement to proceed, finding the SEC adequately alleged the company made false claims about following the NIST Cybersecurity Framework, using secure development practices, and maintaining proper access controls.	Claims regarding statements in press releases, blog posts and podcasts were dismissed as "non-actionable corporate puffery" that lacked the detail a reasonable investor would rely on for investment decisions.	The court dismissed claims about SolarWinds' risk factor disclosures, finding they set out "in stark and dire terms" the "unique risks" the company faced as a cybersecurity provider.	The court found that the SEC's claims regarding the Form 8-K disclosures were also insufficient, as they were protected by the PSLRA's safe harbor for forward-looking statements

Legal Issues: The Security Statement

Access Control Problems

The court found SolarWinds “blatantly contradicted” its Security Statement by providing employees with administrative access on a “largely indiscriminate basis” instead of limiting network access as claimed.

These deficiencies were characterized as “glaring,” “long-standing,” and “well-recognized within the company, yet unrectified over time.”

Password Policy Failures

The court cited evidence that SolarWinds knew its password policy was not enforced in practice, including an incident where a security researcher alerted the company that a password to one of its servers (“solarwinds123”) was publicly available.

These shortcomings were “magnified for SolarWinds” given that cybersecurity was a “key attribute” of the company's products.

Legal Issues: Internal Accounting Controls

The SEC alleged that SolarWinds failed to maintain a system of internal accounting controls sufficient to provide reasonable assurances that access to company assets was permitted only in accordance with management's general or specific authorization, in violation of Section 13(b)(2)(B) of the Exchange Act, and that the CISO aided and abetted the violation.

Section 13(b)(2)(B) requires organizations to implement internal accounting controls that ensure transactions are properly authorized, accurately recorded, assets are protected with controlled access, and regular audits are conducted to reconcile recorded assets against actual assets.

The SEC asserted that "SolarWinds' information technology network environment, source code, and products were among the Company's most critical assets," and thus, when the company was hacked as a result of its allegedly deficient cybersecurity controls, the company violated Section 13(b)(2)(B).

Legal Issues: Internal Accounting Controls

Court's Ruling

The court decisively rejected the SEC's claim that cybersecurity controls fall under "internal accounting controls"

Statutory Interpretation

Section 13(b)(2)(B) is limited to financial accounting controls, not all systems protecting company assets

Implications

Limits SEC's authority to regulate cybersecurity through accounting control provisions

The court found that the SEC's interpretation would have "sweeping ramifications," potentially allowing the agency to regulate everything from "background checks for security guards" to "padlocks for storage sheds." This ruling represents a significant check on the SEC's expanding assertion of enforcement authority beyond financial accounting controls.

Legal Issues: Disclosure Controls and Procedures

The SEC charged SolarWinds with violating Exchange Act Rule 13a-15, which requires companies to maintain a system of disclosure controls and procedures sufficient to ensure that information required to be disclosed is escalated internally to allow for timely disclosure decisions.

The SEC alleged that two cybersecurity incidents preceding the revelation of the Orion compromise, and an earlier discovery of another vulnerability, were not escalated to senior management in accordance with the company's incident response plan.

Legal Issues: Disclosure Controls and Procedures

Court's Ruling

SEC failed to allege systemic deficiencies in controls

Key Finding

Isolated errors don't constitute control failures and incidents did not appear to be significant at the time they occurred. They're only significant with the benefit of hindsight.

Implications

Companies can't be held liable unless there are serious deficiencies in controls and procedures.

The court emphasized that "errors happen without systemic deficiencies" and that the SEC's claim "has traction only with the benefit of post-incident hindsight." This ruling provides important protection for companies making good-faith disclosure decisions during rapidly evolving cybersecurity incidents.

Implications for CISOs and Corporate Officers

Relief for CISOs

The dismissal of most charges against the CISO provides reassurance to security professionals concerned about personal liability. The court noted the irony that the SEC alleged the CISO concealed risks while simultaneously using evidence that he repeatedly raised concerns.

Caution on Public Statements

The surviving claim about the Security Statement underscores the importance of ensuring accuracy in all public-facing security claims, even those outside formal securities filings.

Expanded Review Process

Companies should ensure statements by technical leaders like CTOs, CIOs, and CISOs receive the same vetting as those from other senior executives.

Recognition of Real-Time Challenges

Acknowledges difficulty of perfect disclosure during evolving incidents. disclosures must be evaluated based on information available in real-time, not with hindsight bias. For public companies, this offers some protection when making good-faith disclosure decisions during rapidly evolving cybersecurity incidents.

Protection for Reasonable Disclosure Systems

Isolated errors don't constitute control failures.

Questions

Presenters

Andrew Dawson is a first-chair trial lawyer and former federal prosecutor. Prior to returning to Keker, Van Nest & Peters, he served for nine years at the U.S. Attorney's Office for the Northern District of California, leading and supervising a wide range of white-collar criminal matters and sophisticated transnational investigations. His practice focuses on responding to government investigations and prosecutions, conducting internal investigations, and leading trial teams in matters before juries, judges, and arbitrators.

Puja Parikh's represents clients in all facets of intellectual property and complex commercial litigation. She regularly litigates patent, trade secret, and copyright matters in federal court. Among her recent engagements, Puja served as trial counsel for Dexcom in a complex patent dispute, trial counsel for Meta in a patent infringement suit, and she obtained a permanent injunction on behalf of Instacart in a plaintiff-side copyright lawsuit.

Melissa Cornell represents clients in high-stakes complex civil and criminal litigation, in federal and state court as well as arbitration. In particular, she has recent experience representing technology and media-based companies facing contract, trade secret, and privacy claims. Melissa has also helped clients navigate sensitive internal and government investigations, successfully avoiding costly litigation.

Thank you!