IAA Investment Adviser Compliance Conference 2022
March 3-4, 2022

Data Privacy Overview Panel: Friday, March 4, 11:20 am ET – 12:10 pm ET

I. ***The Emergence of State Comprehensive Privacy Laws***

A. California

1. CCPA Passed in 2018; Effective 2020; Will be updated/replaced with CPRA 2023

2. GLBA data-based exemption

B. Colorado

1. GLBA entity-based exemption

2. Proposals to amend Colorado Privacy Act (CPA) to "strike the appropriate balance between consumer protection and not stifling innovation."

C. Virginia

1. GLBA entity-based exemption

2. Virginia lawmakers propose bills to amend the Virginia Consumer Data Protection Act's right to delete and enforcement provisions.

D. Next? At least 17 states with privacy legislation pending.

II. ***Developing AI Policy and Impact to IAs***

A. Legislation

1. Sept 2021 - Department of Commerce established the National Artificial Intelligence Advisory Committee (NAIAC), which "advise the President and other federal agencies on a range of issues related to artificial intelligence."

2. October 2021 - White House announces it will develop AI Bill of Rights https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/

3. In the National Defense Authorization Act for 2021, Congress directed the National Institute of Standards and Technology (NIST), which falls under DoC, to develop "a voluntary risk management framework for trustworthy AI systems."

4. Algorithmic Accountability Act due to be reintroduced in 2022

5. GAO recommends regulators better protect personal information.

B. Regulation

1. FINRA's June 2020 AI report provides overview of broker-dealers' use of AI applications related to: (i) communications with customers; (ii) investment processes; and (iii) operational functions; and also discusses key factors including potential regulatory considerations, securities market participants may want to consider as they develop and adopt AI-based tools

2. March 2021: The Fed, CFPB, FDIC, NCUA and OCC request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning

3. April 2021 Federal Trade Commission (FTC) published a blog post entitled "Aiming for truth, fairness, and equity in your company's use of AI" (FTC Memo). The FTC Memo makes it clear that the FTC will use its authority under Section 5 of the FTC Act, as well as the Fair Credit Reporting Act (FCRA) and the Equal Credit Opportunity Act (ECOA) to pursue the use of biased algorithms (April 2021)

4. December 2021, FTC prepares for robust rulemaking on privacy and artificial intelligence that will begin with an Advanced Notice of Proposed Rulemaking in February 2022

5. FTC Advanced Notice of Proposed Rulemaking for Trade Regulation in Commercial Surveillance

    a. FTC is also considering promulgating rules to curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination. Public comment closes February 2022.

    b. https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69

6. UK government rolls out global AI standards initiative to "improve the governance of AI, complement pro-innovation regulation and unlock the huge economic potential" following the U.K.'s departure from the EU.

7. Spain's government is budgeting for the creation of the first national AI supervisory authority among EU member states by 2023

8. European Union presented a grand proposal to regulate artificial intelligence based on the potential impact of the AI app

III. ***Developing Consumer Privacy Policy and Impacts to IAs***

A. Regulatory Scrutiny

1. Jan 2021 - CFPB's "Taskforce on Federal Consumer Financial Law Report" (2021) makes recommendations on improving consumer financial privacy through over 100 recommendations to policymakers and regulators.

2. August 2021 - SEC review of broker-dealer and investment adviser "digital engagement practices" (DEPs), features commonly referred to as the "gamification" of trading.

3. Comments period recently ended; rulemaking proposed in 2021.

4. Sept. 2021 - FINRA conducts sweep of how firms supervise activities and communications related to paid social media "Finfluencers"

   a. "firm practices related to the acquisition of customers through social media channels and how firms manage their obligations related to information collected from those customers and other individuals that may provide data to firms."

   b. Requests firms provide their written supervisory procedures concerning its compliance with the SEC's Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information (Regulation S-P), as well as the collection of Cookies obtained from customers, or individuals who provide NPI but are not onboarded as customers.

   c. Also requesting privacy policies and detailed information about data sharing.

B. Continuing interest in privacy legislation

1. E.g., U.S. Reps. and Senator introduce the Banning Surveillance Advertising Act

2. Increased scrutiny and enforcement of GDPR and ePrivacy Directive in the EU

3. India's Personal Data Protection Bill under consideration

IV. ***Focus on Data Protection Compliance Programs – Safeguarding NonPublic Personal Information***

A. Securities Exchange Commission

1. On February 9, 2022, SEC Proposed New Adviser Cybersecurity Reporting and Disclosure Requirements

a. Requiring advisers to confidentially report "significant" cybersecurity incidents to the SEC on new Form ADV-C within **48 hours** after having a reasonable basis to conclude that a significant cybersecurity incident occurred or is occurring;

b. Requiring advisers and funds to adopt and implement written **policies and procedures** that are reasonably designed to address cybersecurity risks

c. Enhancing adviser and fund **disclosures** related to cybersecurity risks and incidents that occurred in the past two years in a new Item in Form ADV Part 2A

d. Requiring advisers and funds to maintain, make, and retain certain cybersecurity-related **books and records**

2. Enhanced focus on cybersecurity policy through the lens of the Safeguards Rule / Reg S-P

a. In August 2021, the SEC announced that it had fined eight broker-dealers and investment companies for their "deficient cybersecurity procedures."

b. Repeated Business Email Compromises leading to compromise of thousands of clients' personal data – SEC found policy violations

c. The SEC's order also alleged certain breach notifications included misleading language suggesting that the notifications were issued much sooner than they actually were after discovery of the incidents, in violation of Section 206(4) of the Advisers Act and Rule 206(4)-7.

d. Kristina Littman, Chief of the SEC Enforcement Division's Cyber Unit: "It is not enough to write a policy requiring enhanced security measures if those requirements are not implemented or are only partially implemented, especially in the face of known attacks."

3. SEC encourages Self-Reporting of Recordkeeping Violations Resulting From Employees' Use of Personal Devices for Business Communications

a. December enforcement related to registrants maintaining and preserving employees' business-related communications outside of the firm's channels ("off-channel communications.") Those communications can occur on employees' personal devices, using text messages, messaging applications or personal email accounts.

b. The Enforcement Division also recently launched an enforcement sweep to investigate registered broker-dealers' off-channel communication retention practices.

B. Federal Trade Commission

1. Gramm-Leach-Bliley Act (GLBA) Safeguards Rule:

a. FTC updates to the GLBA Safeguards Rule (Oct. 2021)

b. https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial

c. More stringent technical cybersecurity requirements

d. Additional governance requirements

e. Need for enhanced policies

2. Supplemental Notice of Proposed Rulemaking proposes to further amend the Safeguards Rule

a. Potential new FTC breach notification?

b. Within 30 days, with risk of harm (misuse) and 1000+ impacted person trigger; public database of notices.

c. "Such reports would ensure the Commissioner is aware of security events that could suggest a financial institution's security program does not comply with the Rule's requirements, thus facilitating Commission enforcement of the Rule."

d. December 2021 NPRM Comment Period Closed Feb 7, 2022

e. https://www.federalregister.gov/documents/2021/12/09/2021-25064/standards-for-safeguarding-customer-information

C. Trending Cybersecurity Topics

1. Supply Chain Vulnerabilities and Nation State Attacks

a. Solar Winds

b. Log4J

c. Russia

2. SEC Chairman Gary Gensler looking to expand and modernize SEC's regulatory framework around cybersecurity in the financial sector (Jan. 2022)

a. Agency's rules will implicate cyber risks, particularly as they relate to business continuity, books and records, disclosures, market access and fraud protection.

b. Registrants not covered by Reg SCI could benefit from reforms that reduce the risk of disruptions from significant cybersecurity incidents, Gensler said.

c. Regulation S-P, which requires broker-dealers and investment companies to safeguard customer records, could be expanded so that customers and clients receive notifications when their data has been illegally accessed.

d. SEC staff are also putting together recommendations for a consistent cyber risk disclosure framework for public companies and a protocol for updating investors when cyber events occur

D. New York Department of Financial Services

1. Enforcement Trends

2. New Guidance on multi-factor authentication and cybersecurity frameworks

3. https://www.dfs.ny.gov/industry_guidance/industry_letters/il20211207_mfa_guidance