



Emerging Privacy and Cybersecurity Issues to Look for in 2024

FTC's Focus on Health Data

The FTC increased its focus on applications collecting and processing health data. The FTC specifically focused on disclosures made to consumers regarding the selling and sharing of health data and whether the company was abiding by those promises. It is anticipated that the FTC will continue its focus on ensuring companies collecting health data are being transparent with consumers.

FTC's Focus on Children's Data

Children's data received increased attention by the FTC and by state and federal legislators in 2023. Collection, processing, and sharing of children's data are being scrutinized and will likely continue to be an area of regulatory focus in 2024.

FTC's Focus on Biometric Data Processing

The Federal Trade Commission (FTC)'s policy statement on unfair practices in processing biometric data and its anticipated enforcement actions in 2024 highlight a growing regulatory focus on this area.

GLBA Safeguard Rule

New breach reporting requirements for non-bank financial institutions.

SEC Requirements for Public Companies

Require public companies to disclose both material cybersecurity incidents they experience and, on an annual basis, material information regarding their cybersecurity risk management, strategy.

Data Transfers and International Regulations

With the new EU Data Act and other global developments, companies will need to navigate stricter data transfer regimes and local data hosting requirements, especially in critical infrastructure sectors.

General Privacy and Data Protection Litigation in the EU

An increasing number of privacy litigation cases in the EU, particularly focusing on how companies handle user data, consent, and privacy violations.

China's Privacy Laws

China's evolving privacy regulations, especially under the Personal Information Protection Law (PIPL) and the Data Security Law (DSL), will continue to impact international businesses operating in or with China.

New Privacy Laws in Asia, Africa, and the Middle East

Many jurisdictions in these regions are expected to continue adopting and revising privacy laws, focusing on broadening jurisdictional scope and imposing more stringent data security obligations.

Data Privacy Issues in the Automobile Industry

As vehicles become smarter, they collect more personal information. Vehicle manufacturers share personal information and consumers often have little control over personal data. This may be an area of regulatory focus in 2024.

Emergence of Neuroprivacy

As technology advances, devices that can read and write to the mind pose new privacy challenges, raising questions about the rights individuals have to their inner thoughts and feelings.

Increasing Focus on Data Collaboration and Privacy-Centric Solutions

The rise in data collaboration and the development of privacy-centric cloud-native solutions is an emerging trend. This approach aims to facilitate data connectivity without creating additional data silos, enhancing privacy and security.

Election Security

With the United States entering an election year, there will be increased focus on protecting the integrity of the electoral process from cyber threats. This includes safeguarding government systems, polling locations, and third-party systems involved in the election process.

Incentivized Cybersecurity

A shift towards incentivized cybersecurity is anticipated, where organizations are rewarded for implementing proper cybersecurity protections and resilience strategies.

Individual Accountability in Cybersecurity

There will be a trend towards holding individuals, especially in executive roles, accountable for organizational cybersecurity incidents.

Organizational Transparency in Cybersecurity

Organizations will be under pressure to disclose cybersecurity incidents early, driven by regulatory requirements like the SEC's cybersecurity reporting rules.

Zero-Trust Architecture

A widespread adoption of Zero-Trust Architecture as organizations move away from traditional perimeter-based security. This involves verifying every user and device attempting to access network resources.

Increased Regulatory Fines in Australia Australian regulators are expected to start issuing significant fines to organizations that fail to implement appropriate cybersecurity controls.

SEC Cybersecurity Rules

The new SEC cybersecurity rules, effective from December 2023, have raised concerns among senior management about the level of detail to disclose in annual filings and information sharing with the board. This could lead to changes in how public companies describe their cybersecurity incidents practices and risks.

EU's Cyber Resilience Act

The draft Cyber Resilience Act (CRA) is expected to gain traction in 2024. It aims to bolster the cybersecurity posture of connected products and services in the EU market. Companies will need to adapt to the new cyber framework regarding applicability and requirements.

EU Data Act

The Act will become enforceable in 2025, and applies to a variety of entities including (i) manufacturers of connected products, (ii) suppliers of related services; (iii) "data holders" that have the right or obligation to use or make data available; and (iv) providers of data processing services covers both personal and non-personal data that is obtained, generated, or collected by connected products and/or their components, and related digital services.

Implementation of NIS 2 Directive

In the EU, the NIS 2 Directive is set to be transposed into national laws of EU member states by October 2024. This directive introduces new cybersecurity obligations related to security and incident reporting. Its broader scope affects both EU and non-EU organizations, necessitating a reassessment of cybersecurity practices.

Rise in Bug Bounties

An increase in the use and reward of bug bounties, particularly for vulnerabilities specific to artificial intelligence, is expected as a means to enhance cybersecurity.

AI's Role in Cybersecurity Threats and Defenses

The dual role of AI in both enhancing cybersecurity defenses and being used as a tool for sophisticated cyber attacks is a significant trend. This includes AI's use in phishing attacks, which are becoming more complex and harder to detect.

Smart City Infrastructure and IoT Risks

The integration of IoT and connected systems into city infrastructures in the APAC region and globally will increase cybersecurity risks, particularly for critical operations.

Supply Chain Cybersecurity Risks

Managing supply chain risks will become a top priority, with organizations scrutinizing their suppliers' cybersecurity practices and developing contingency plans.

Cybercrime and Re-extortion

Cybercrime is increasingly becoming a volume business. Even when cybercriminals promise to delete stolen data, the threat of re-extortion over exfiltrated data is a growing concern. This suggests that data breaches could have longer-term repercussions than previously anticipated.

Connected and Electric Cars Cyber Attacks

With the increasing number of connected and electric vehicles, there is an anticipated rise in targeting auto manufacturers' supply chains and infrastructure for cyberattacks. This also includes growing regulatory requirements focused on automotive data privacy and law enforcement requests for driver and vehicle-related information.

Cyberbullying and Deepfake Technology

An increase in cyberbullying, particularly using deepfake technology, is anticipated. This trend involves manipulating publicly available images to create false and potentially harmful content, posing significant risks to privacy and well-being, especially for young adults and children.

Charity Fraud and AI-Enabled Scams

There is an expectation of a rise in charity fraud and AI-enabled scams. Scammers are likely to exploit emotions like empathy and grief, using advanced AI tools to fabricate convincing scams, thereby endangering consumer privacy and security.

QR Code Scams (Qishing)

The rise of malicious QR codes, leading to phishing websites or triggering malware downloads, is a growing concern. This trend underscores the need for vigilance in mobile and digital interactions.

Olympic Scams

Major global events like the Olympic Games are expected to become hotspots for cyber scams, with cybercriminals exploiting consumer enthusiasm to compromise personal information and payment details.

Sexual Harassment and Grooming in Digital Platforms

The issue of sexual harassment and grooming, including in virtual reality environments, is gaining attention. The integration of security by design into a broader assessment of safety by design is expected to address these concerns.