

**Privacy Regulation Roundup – February 2024**

This Privacy Regulation Roundup summarizes the latest major global privacy regulatory developments, announcements, and changes. This report is updated on a monthly basis. For each relevant regulatory activity, you can find actionable Info-Tech analyst insights and links to useful Info-Tech research that can assist you with becoming compliant.

Contents

[Google Research Reveals Global Spyware Threat 3](#_Toc159522366)

[Type: News 3](#_Toc159522367)

[Date: February 2024 3](#_Toc159522368)

[California Cracks Down on Mobile App Data Practices 4](#_Toc159522369)

[Type: Regulations 4](#_Toc159522370)

[Announcement Date: January 2024 4](#_Toc159522371)

[Alberta Looking to Improve Privacy Protection Within the Next Two Years 5](#_Toc159522372)

[Type: Announcement 5](#_Toc159522373)

[Announcement Date: January 2024 5](#_Toc159522374)

[“Mother of all Breaches” Exposes Over 26 Billion Personal Records 6](#_Toc159522375)

[Type: News 6](#_Toc159522376)

[Date: January 2024 6](#_Toc159522377)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Google Research Reveals Global Spyware Threat

## Type: News

## Date: February 2024

**Summary:** In a recent report, Google casts light on the substantial risks commercial surveillance vendors pose to global users. The internet giant urges the United States and its allies to take more decisive action in reining in the spyware industry.

Spyware firms offer comprehensive solutions for bypassing security measures and continue to claim that their products are intended for government use in national security efforts. However, the report details the operations of 40 commercial spyware vendors, emphasizing the industry’s role in distributing harmful hacking tools and exploiting vulnerabilities for surveillance. These tools find their way into the hands of a collaborative ecosystem of state and non-state actors that includes vulnerability researchers, exploit developers, and government clients. These groups deploy spyware against journalists, human rights defenders, dissidents, and opposition politicians.

Google plays a proactive role in disrupting the spyware ecosystem by identifying and fixing vulnerabilities, sharing intelligence, and offering advanced protection for high-risk users.

**Analyst Perspective:** The use of spyware is not limited to counterterrorism or law enforcement but is increasingly used to undermine free speech, press freedom, and election integrity. Organizations that operate in high-risk jurisdictions, engage in high-risk activities, or support the travel of high-risk users should heed the report’s call to action.

* Define the risk scenario you face carefully, including the assets at risk, their vulnerabilities, and the threat actors that would exploit them.
* Next, assess the inherent risk users face, identify existing controls, and consider additional controls that you might put in place to improve your security posture.

Finally, put in place vulnerability management and threat intelligence gathering programs to support ongoing efforts to protect users from the pervasive threat of commercial spyware.

**Analyst:** [Michel Hebert](https://www.infotech.com/profiles/michel-hebert), Principal Research Director – Security & Privacy

**More Reading:**

* Source Material: [Forbes](https://www.forbes.com/sites/daveywinder/2024/02/06/new-google-warning-reveals-global-2024-privacy-threat-are-you-at-risk/?sh=724f4c2a283c), [Google](https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors.pdf), [SiliconANGLE](https://siliconangle.com/2024/02/06/google-report-warns-risk-posed-commercial-surveillance-industry/), [EconoTimes](https://www.econotimes.com/Google-Calls-Out-Surveillance-Software-Companies-Enabling-Dangerous-Hacking-Tools-1671026)
* Related Info-Tech Research:
* [*Secure Operations in High-Risk Jurisdictions*](https://www.infotech.com/research/ss/secure-operations-in-high-risk-jurisdictions)
* [*Implement Risk-Based Vulnerability Management*](https://www.infotech.com/research/ss/implement-risk-based-vulnerability-management)
* [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# California Cracks Down on Mobile App Data Practices

## Type: Regulations

## Announcement Date: January 2024

**Summary:** On January 27, 2023, California Attorney General Rob Bonta initiated an investigative sweep targeting mobile apps, particularly in retail, travel, and food service sectors. This sweep focused on apps suspected of violating the CCPA by:

* Lacking opt-out mechanisms: Not providing users with a way to opt out of personal data sales.
* Ignoring authorized agent requests: Failing to process opt-out requests submitted through designated agents.

This action highlights the AG’s commitment to enforcing the CCPA, considered one of the strictest privacy laws in the US. It follows a similar case against Sephora in August 2022, where the company settled allegations of non-disclosure of data sales and failure to honor user-enabled opt-out controls. Additionally, the AG launched a reporting tool for consumers to flag potential CCPA violations.

**Analyst Perspective:** Mobile app developers, especially in the targeted industries, should review their CCPA compliance measures, particularly opt-out mechanisms, and authorized agent protocols. This sweep signifies the growing focus on data privacy enforcement, urging businesses to prioritize user control over personal information. The AG’s actions emphasize the importance of transparency and respecting user opt-out choices, regardless of the request channel.

**Analyst**:[Carlos Rivera](https://www.infotech.com/profiles/carlos-rivera), Principal Advisory Director – Security, Privacy, Risk & Compliance

**More Reading:**

* Source Material: [Department of Justice](https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-investigative-sweep-focuses-streaming-services%E2%80%99), [The National Law Review](https://www.natlawreview.com/article/california-attorney-general-announces-industry-investigative-sweep-ccpa-compliance), [Goodwin’s Data, Privacy + Cybersecurity Insights Blog](https://www.goodwinprivacyblog.com/2023/01/30/california-attorney-general-announces-focus-on-mobile-apps/#:~:text=On%20January%2027%2C%202023%2C%20California%20Attorney%20General%20Rob,on%20the%20retail%2C%20travel%2C%20and%20food%20service%20industries.)
* Related Info-Tech Research:
  + [*Comply With the California Consumer Privacy Act*](https://www.infotech.com/research/ss/comply-with-the-california-consumer-privacy-act)
  + [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
  + [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Alberta Looking to Improve Privacy Protection Within the Next Two Years

## Type: Announcement

## Announcement Date: January 2024

**Summary:** The province of Alberta is looking to improve its privacy protections for Albertans within the next 18 months. The announcement was made during late January, by the Minster of Technology and Innovation Nate Glubish. The Ministry will look into improving their privacy protections by implementing their new Data Ethics and Privacy Management framework, which focuses on the management and use of data ethically within the government, with emphasis on protecting Albertans’ personal information. The proposal includes the launch of various initiatives, including proposals to amend Alberta’s privacy legislation that will ensure the penalties they have in place for the misuse of Albertans’ data and violation of their privacy will be one of the strongest in Canada. This comes under the Ministry’s strategy to ensure that every technology, service, and system used within the government will adhere to the principles developed by the province. Although this plan is still in its initial stages, it has already been reviewed and gained support from the Office of the Information and Privacy Commissioner of Alberta.

**Analyst Perspective:** With many government agencies implementing strategies to improve their privacy program, including in the US, it has been known that Canadian government agencies would also follow suit. With over 93% of Canada’s population using the internet, it is important that the various government agencies are focusing on improving their privacy protection to ensure their citizens can safely access necessary services without the concern of their data being misused. The announcement by the province of Alberta could be a first step in formalizing an effective data privacy program that can be iteratively reviewed to align its protection measures with the evolving technologies being developed. This could influence other provinces and territories within the country to also review their privacy protection measures in place to ensure their citizens are continuing to have confidence in their data being protected.

**Analyst:** [Ahmad Jowhar](https://www.infotech.com/profiles/ahmad-jowhar), Research Analyst – Security & Privacy

**More Reading:**

* Source Material: [DiscoverAirdrie](https://discoverairdrie.com/articles/province-looking-to-clamp-down-on-data-privacy), [LethbridgeNewsNOW](https://lethbridgenewsnow.com/2024/01/26/alberta-strengthening-privacy-protections-for-residents/), [IAPP](https://iapp.org/news/a/alberta-promises-increased-privacy-protections-in-next-18-months/), [DataReportal](https://datareportal.com/reports/digital-2023-canada#:~:text=Canada%27s%20internet%20penetration%20rate%20stood,percent)%20between%202022%20and%202023.)
* Related Info-Tech Research:
* [*Build a Data Privacy Program*](https://www.infotech.com/research/ss/build-a-data-privacy-program)
* [*Mature Your Privacy Operations*](https://www.infotech.com/research/ss/mature-your-privacy-operations)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# “Mother of all Breaches” Exposes Over 26 Billion Personal Records

## Type: News

## Date: January 2024

**Summary:** In January 2024, security researchers unearthed a colossal database of leaked data totaling 12 terabytes, earning the title “Mother of All Breaches” (MOAB). While the perpetrator remains unidentified, the database is believed to have been compiled by malicious actors or data brokers. The massive 26 billion records include data from major platforms like Tencent, Weibo, Twitter, Dropbox, and LinkedIn. More alarmingly though, records from various US and other government organizations were also identified in the database.

This raises concerns about identity theft, sophisticated phishing schemes, and unauthorized access to accounts. Additionally, the presence of usernames and passwords further increases the risk of credential stuffing attacks. While this discovery is worrying, at an individual level adhering to best practices in password management and security measures, such as enabling two-factor authentication for all accounts, can mitigate risks.

**Analyst Perspective:** Private and public organizations should take note that profiles built using such large data sets can be used for spear phishing and other socially engineered attacks against key players in the senior management or executive suite. Moreover, whether employees are using personal credentials to access generative AI services, for boosting productivity, warrants due consideration as that could leave confidential business information at higher risk of exposure.

This is a wake-up call for organizations and institutions, reminding them that prioritizing data privacy and security is ever so important. Implementing comprehensive data protection policies and procedures, aligned with privacy laws such as the GDPR and CCPA, can help mitigate legal risks associated with data breaches. Additionally, investing in cybersecurity infrastructure including employee training, multi-factor authentication, robust encryption mechanisms, access controls, incident management, and regular security audits helps organizations minimize vulnerabilities and reduce the risk landscape.

**Analyst:** [Safayat Moahamad](https://www.infotech.com/profiles/safayat-moahamad), Research Director – Security & Privacy

**More Reading:**

* Source Material: [Forbes](https://www.forbes.com/sites/daveywinder/2024/01/23/massive-26-billion-record-leak-dropbox-linkedin-twitterx-all-named/?sh=4ac2b6f3ab58), [DailyMail](https://www.dailymail.co.uk/sciencetech/article-12992157/Huge-data-leak-dubbed-Mother-Breaches-sees-26-BILLION-records-leaked-sites-including-Twitter-Linkedin-Dropbox-heres-check-youve-affected.html), [IAPP](https://iapp.org/news/a/26-billion-data-record-trove-gets-mother-of-all-breaches-designation/)
* Related Info-Tech Research:
* [*Fast Track Your GDPR Compliance Efforts*](https://www.infotech.com/research/ss/fast-track-your-gdpr-compliance-efforts)
* [*Comply With 2023 US Privacy Laws*](https://www.infotech.com/research/ss/comply-with-2023-us-privacy-laws-virginia-connecticut-utah-colorado)
* [*Build a Security Compliance Program*](https://www.infotech.com/research/ss/build-a-security-compliance-program)
* [*Address Security and Privacy Risks for Generative AI*](https://www.infotech.com/research/ss/address-security-and-privacy-risks-for-generative-ai)