BixeLab

29 January 2025

I.D. RISK ALERTS

Open Source Edition

Identity and Biometric Vulnerabilities | Threats and Risks | Mitigations

Welcome

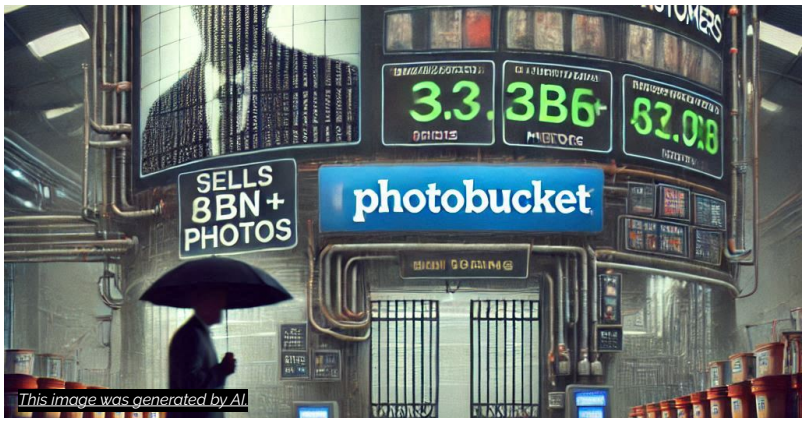
The I.D. Risk Alerts newsletter (open source edition) is a quarterly newsletter with analysis on recent ID fraud, biometric threats and identity vulnerabilities that are already known in the public domain. A comprehensive bi-annual report will also be available to select BixeLab subscribers.

EU's Giant Leap and Its Implications for Travel

The European Union is on the verge of housing the largest biometric data repository globally, a move integral to shaping a 'fully digital travel experience'. The International Air Transport Association (IATA) highlights biometrics and digital identities as transformative tools making passport-free travel a tangible possibility, though legislative processes are yet to synchronise with technological advancements. Norway is taking proactive steps by planning the deployment of 21 biometric border control gates, emphasising increased security and efficiency at borders. Concurrently, Malta's 2025 budget suggests a tender for a digital ID wallet, signifying broader moves within the EU to bolster digital identity mechanisms. While these advancements promise enhanced convenience for travellers, they also raise concerns regarding privacy and data management.

Legislative Changes and Tech Initiatives

Emerging AI oversight initiatives in the United States face potential uncertainties as future President Trump's deregulation plans could impact proposed bills and guidance intended to bolster governance of AI technologies. At the same time, Meta is enhancing safety measures on its social media platform by introducing new age-checking protocols and "teen" accounts for young Instagram users. These measures aim to protect adolescents from inappropriate content and interactions, highlighting an increased focus on safeguarding youth online amidst evolving regulatory landscapes.



Photobucket Faces Legal Backlash Over Unauthorised Use of Biometrics in AI Training

Modality: **Face, Iris** Attack Instrument: **Unauthorised Data Sale**
Location: **U.S. (Illinois, NY, California)** Date of report: **Dec 2024**

A lawsuit has been filed against Photobucket after a privacy policy update revealed plans to sell users' photos, including biometric identifiers such as face and iris scans, to AI companies without obtaining explicit consent. This lawsuit alleges Photobucket failed to adhere to strict state privacy laws in the US by selling biometric data without user consent, affecting potentially **100 million** users. The collection, which includes over **13 billion** photos, has been partially identified for AI licensing purposes. Plaintiffs include both a mother of a minor and a professional photographer, both concerned about their biometric data being sold. The lawsuit could result in substantial penalties, amounting to **$5,000** per violation.

- **Potential Targets:** users of platforms like Photobucket, whose biometric data, uploaded unknowingly or without updated consent, are at risk.
- **Mitigation Strategy**: implementing strong consent protocols, ensuring explicit opt-in consent for any sale or usage of biometric data. This is conducted through thorough audits of data transaction processes, reinforcing transparency in privacy policy updates, and endorsing independent privacy impact assessments (PIAs) for compliance with legal standards.
- **Criticality: High** -the unauthorised sale and potential misuse of biometric data, including its potential role in developing advanced AI systems capable of deepfake creation. This poses severe risks to individual privacy and elevates the critical urgency for robust data protection measures and legislative compliance.

Advancing Digital Identity and Governance in Southeast Asia

The Philippines is taking a significant step in enhancing its Know Your Customer (KYC) capabilities by introducing a new postal ID card. This move aims to streamline identity verification processes, leveraging biometric technologies to bolster security and efficiency. Concurrently, Thailand is advancing its digital identity framework into its second phase, which is set to enhance digital identity verification and facilitate secure online transactions. In Malaysia, the government is on track to complete its digital governance ecosystem by early 2025, a move expected to integrate various public services into a unified digital platform. Meanwhile, Singapore is pioneering a passport-less immigration clearance system, utilising facial and iris recognition to expedite the entry process and increase security. BixeLab is delighted with the success of our recent webinar titled "Navigating the Emerging APAC Market for Digital ID." For further insights into the region, we recommend reading Dr. Dunstone's recent Medium article.

Launch of New Zealand's Digital Identity Services Trust Framework

New Zealand marks a significant milestone in its digital evolution with the launch of the Digital Identity Services Trust Framework. This framework aims to provide a robust and secure system for managing digital identities, ensuring trust and privacy for users. By establishing clear guidelines and standards for digital identity services, New Zealand seeks to enhance the security and efficiency of digital interactions for citizens and businesses alike. The BixeLab team is proud to have played a role in this initiative through our provision of demographic bias evaluation services to the NZ Department of Internal Affairs' DIA's Identity Check web application. You could also read the full report here.

Transitioning to Biometrics: NAB's Move Beyond Passwords in Online Banking

The National Australia Bank (NAB) is set to overhaul its online banking security by phasing out traditional passwords in favour of biometric authentication methods. This significant shift aligns with the digital transformation trends seen across industries, aiming to enhance security and streamline user experience. As customers embrace the digital boom, the adoption of biometrics like fingerprint and facial recognition seeks to provide a more secure, efficient, and personalised banking experience, minimising the risks associated with password breaches.

Prohibition on Commercial Exploitation of Biometric Data in Brazil

Modality: **Iris** Attack Instrument: **Financial incentives for biometric data** Location: **Brazil** Date of report: **Jan 2025**

Brazilian regulators have taken action against Tools for Humanity (TFH), halting the company's initiative of providing cryptocurrency to citizens in return for their personal iris scans. TFH, co-founded by OpenAI CEO Sam Altman, has faced scrutiny regarding cryptocurrency payments in exchange of biometric data, as it severely influences an individuals independent and informed decision making process regarding sharing their sensitive biometric data. The National Data Protection Authority (ANPD) expressed concern over the ethical implications, citing vulnerability and the potential for coercion due to financial restraints. The ban has been in effect since 25th January 2025. TFH has responded, asserting compliance with all Brazilian regulations and is actively engaging with the ANPD to resolve the situation.

- **Potential Targets:** general population, particularly those in financial need, could be targeted through coercive means to collect sensitive biometric data. This presents a risk in the integrity of biometric systems by potentially overpowering an individual's will to consent freely and independently.
- **Mitigation Strategy:** re-evaluate and tighten regulations surrounding the exchange of financial rewards for biometric data. Implement comprehensive independent biometric testing and verify that all processes adhere to national data protection laws. Educate the public on the importance of informed and voluntary consent regarding the sharing of biometric details. Enhance live testing procedures to ascertain authenticity and bolster privacy safeguards.
- **Criticality:** **Medium** - the intersection of financial incentives with biometric data collection posits significant privacy and ethical challenges. The exploitation of personal biometric information under coercive circumstances is a serious concern, necessitating robust regulatory measures and public awareness initiatives.

Infiltration of US Telecommunications by 'Salt Typhoon'

Modality: **Communications Infrastructure** Attack Instrument: **Cyber espionage** Location: **U.S.** Date of report: **Nov 2024**

Recent cyber espionage activities attributed to the Chinese government-linked hacker group, Salt Typhoon, have highlighted significant vulnerabilities within the US telecommunications sector. This attack has primarily targeted major telecommunications companies such as AT&T, Lumen, and Verizon, which are essential for government and law enforcement communications, including systems supporting court-ordered wiretaps as per the Communications Assistance for Law Enforcement Act (CALEA). The breach has exposed the potential interception of sensitive communications and compromised the confidentiality of US intelligence operations. The attacks underline the strategic value these infiltrations hold for foreign governments, particularly regarding intelligence on national policies and diplomatic strategies.

- **Potential Targets:** communication infrastructure used by government and law enforcement agencies, high-value targets including government officials, intelligence services, and senior political figures.
- **Mitigation Strategy:** update telecommunications security standards, enhance encryption measures, establish mandatory audits, enforce rigorous access control, promote collaboration between federal agencies and private telecom operators, and develop proactive counterintelligence measures.
- **Criticality: High** - the infiltration by Salt Typhoon reveals critical deficiencies in current US cybersecurity infrastructure, posing severe national security risks due to the potential access to sensitive government communications and data, which could lead to significant geopolitical and operational repercussions.

Emergence of AI-Driven Cybercrime Tools - FraudGPT and WormGPT

Modality: **Text Generation** Attack Instrument: **Generative AI (FraudGPT, WormGPT)** Location: **Dark Web, Telegram** Date of report: **Jul 2024**

Cybercriminals have embraced AI technology with the introduction of malicious chatbots like FraudGPT and WormGPT, now available on dark web marketplaces. These tools, which mimic popular AI applications, are specifically designed for nefarious activities, including writing malicious code, creating phishing pages, and crafting scam emails. Sold on a subscription basis (starting at $200 per month), FraudGPT claims over 3,000 sales and provides threat actors with the ability to undermine security systems across various platforms by generating undetectable malware, finding vulnerabilities, and learning to code or hack.

- **Potential Targets:** individuals and entities reliant on electronic communication are at greater risk of exposure to AI-generated cyber threats. Businesses using online infrastructure, financial sectors, and individuals susceptible to phishing are particularly vulnerable.
- **Mitigation Strategy:** a robust cybersecurity strategy should be implemented, including extensive monitoring of networks for unusual activity, implementing phishing-resistant protocols, and frequent patching of known vulnerabilities.
- **Criticality: High** - the advent of AI-fuelled cybercrime tools poses a serious threat to cybersecurity. Given their capabilities to execute complex, scalable attacks with refined human-like interactions, the potential for widespread financial loss and data breaches is significant.

AI Deepfake Exploitation in Financial Sector Biometric Systems

Modality: **Face, Image Attack** Attack Instrument: **AI deepfake technology** Location: **Indonesia** Date of report: **Dec 2024**

In a significant breach, a prominent financial institution in Indonesia faced profound financial losses exceeding $135 million USD. Cybercriminals apparently employed deepfake technology to circumvent advanced biometric security measures, including facial recognition and liveness detection, particularly in the Know Your Customer (KYC) onboarding process. By illicitly acquiring victims' IDs, they manipulated images to bypass these biometric verifications successfully, thereby fraudulently obtaining loans with no intention of repayment. Group IB's investigation uncovered over 1,100 deepfake fraud attempts targeting the KYC process. This highlights a global issue with AI-generated text, images, audio, and video being actively used by cybercriminals to strengthen fraudulent schemes. Banks and fintech companies globally are reportedly detecting up to 1,500 deepfake spoofing attacks monthly.

- **Potential Targets:** financial institutions, particularly those utilising biometric technology for KYC processes, remain vulnerable alongside any systems reliant on facial recognition and liveness detection.
- **Mitigation Strategy:** enhance biometric testing and bolster liveness detection mechanisms, conduct regular security audits, incorporate multiple layers of verification beyond biometric confirmations, establish stringent monitoring for unusual transactions, and bolster cybersecurity frameworks to detect and neutralise deepfake attempts.
- **Criticality: Medium** - the breach demonstrates the severe vulnerabilities within biometric security systems posed by advanced AI deepfake technology, necessitating immediate action to safeguard financial systems from escalating cyber threats.