




The New Better: Protecting Data in a Post-Pandemic Age

John Shegerian



iaitam.org | Peace, Love & Asset Management | ACE 2022


1




The World Has an E-Waste Problem
(ERI Featured in Time Magazine)


As a tech-hungry nation flush with cash gets ready to upgrade to the next generation of lightning-fast 5G devices, there is a surprising environmental cost to be reckoned with: a fresh mountain of obsolete gadgets.

- Americans spent \$71 billion on telephone and communication equipment in 2017, nearly five times what they spent in 2010 even when adjusted for inflation, according to the Bureau of Economic Analysis.
- When we buy something new, we get rid of what's old. That cycle of consumption has made electronic waste the world's fastest-growing solid-waste stream. That stream is expected to turn into a torrent as the world upgrades to 5G, the next big step in wireless technology.
- Less than a quarter of all U.S. electronic waste is recycled, according to a United Nations estimate. The rest is incinerated or ends up in landfills. That's bad news, as e-waste can contain harmful materials like mercury and beryllium that pose environmental risks.



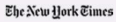
Article: The World Has an E-Waste Problem
Title:
Source: <http://time.com/5594382/world-electronic-waste-problem/>





iaitam.org | Peace, Love & Asset Management | ACE 2022

2



The Price of Recycling Old Laptops

The e-waste industry is booming in Southeast Asia, frightening residents worried for their health. Despite a ban on imports, Thailand is a center of the business.

- Last year, Thailand banned the import of foreign e-waste. Yet new factories are opening across the country, and tons of e-waste are being processed, environmental monitors and industry experts say.
- For years, China took in much of the world's electronic refuse. Then in 2018, Beijing closed its borders to foreign e-waste. Thailand and other countries in Southeast Asia saw an opportunity.
- "Every circuit and every cable is very lucrative, especially if there is no concern for the environment or for workers," said Penchom Saetang, the head of Ecological Alert and Recovery Thailand, an environmental watchdog.
- In Thailand, millions of undocumented workers from poorer countries like Myanmar and Cambodia are vulnerable to abuse, environmental watchdogs say, adding that the need for such laborers will only intensify.



Article: The Price of Recycling Old Laptops: Toxic Fumes in Thailand's Lungs
Title:
Source: <https://www.nytimes.com/2019/12/08/world/asia/e-waste-thailand-lead-acid-batteries.html>





iaitam.org | Peace, Love & Asset Management | ACE 2022

3



4

Environmental Laws

Businesses must be in compliance with varying federal and state e-waste related laws and regulations.

- ✓ **Resource Conservation and Recovery Act (RCRA)**
Federal law that governs the management of hazardous wastes.
- ✓ **State Landfill/Disposal Bans**
19 States and the District of Columbia have a ban on the disposal of some or all electronic material.
- ✓ **Comprehensive Environmental Response, Compensation, and Liability (CERCLA or Superfund)**
Federal law that puts liability of persons responsible for releases of hazardous waste, including generators.
- ✓ **Advanced Recovery Fees (ARF)**
The State of California and 8 Canadian Provinces have a fee on the sale of certain electronic devices to cover the cost of recycling.
- ✓ **State Universal Waste Regulations**
11 States regulate some or all electronic devices as Universal Waste, adding specific storage and management standards.
- ✓ **Extended Producer Responsibility (EPR) Laws**
24 U.S. States, the District of Columbia, and the Province of Ontario have legislation in place requiring manufacturers take responsibility for the End-Of-Life Management of their products.


iaitam.org | Peace, Love & Asset Management | ACE 2022

5

FORTUNE
September 15, 2017
Dead, But Not Forgotten

iaitam.org | Peace, Love & Asset Management | ACE 2022

6



Data Security Laws


ERI's certifications and expert team ensure our clients are in compliance with ever-expanding data destruction global, federal and state laws and requirements.

Existing Legislation


- ✓ HIPAA & HITECH: Healthcare and Business Associates
- ✓ FACTA & FCRA: Businesses that use credit checks or background checks
- ✓ FISMA: Federal Agencies, State Agencies, government contractors, and service providers
- ✓ California Consumer Privacy Act: All for-profit businesses having data on any CA resident
- ✓ FTC ACT: Businesses with a data privacy policy
- ✓ GLBA: Banking, Financial Services, Insurance, and many other organizations
- ✓ PCI DSS: Card Processors and Service Providers
- ✓ COPPA: Sites that collect data on children
- ✓ FERPA: Federally funded schools (under an applicable program of the U.S. Department of Education)
- ✓ GDPR: Companies that handle personal information of an individual in the EU
- ✓ NYS DFS Cybersecurity Regulations: Financial companies doing business in New York
- ✓ Additional State Laws: State specific data security legislation in all 50 states
- ✓ Critical Infrastructure Protection: Power Generation, Oil & Gas, Telecommunications

New Legislation

- ✓ Nevada: SB228 allows consumers to opt out of the sale of their personal information by website operators.
- ✓ California: California Privacy Act provides consumers wide ranges of rights on knowledge, access, and management of their data.
- ✓ New York: The SHIELD Act expanded NY's breach notification requirements and mandates reasonable safeguards to all business entities.
- ✓ Maine: Act to Protect the Privacy of Online Consumer Information requires consumers opt-in to the use or sale of their data from internet service providers.
- ✓ Colorado: Colorado Privacy Act puts the responsibility of data protection and management on companies that control or process Colorado residents' data.
- ✓ Virginia: COPA provides consumers with six main rights and establishes a framework for controlling and processing personal data in the Commonwealth.



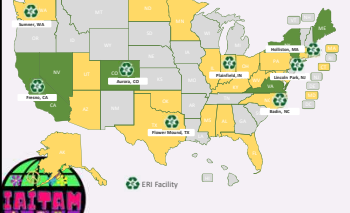
iaitam.org | Peace, Love & Asset Management | ACE 2022



7

New and Proposed Data Security Laws

All 50 states have data security regulations in addition to federal laws. Since the implementation of GDPR in Europe (May 25, 2018), 6 states have passed new legislation, and at least 22 states have recently proposed new legislation or have enacted study bills. In addition, at least 25 US federal laws and regulations are currently proposed. Internationally, at least 6 countries have passed or updated legislation and at least 3 major countries have proposed federal legislation.




New Legislation


- California – CCPA/CPRA
- Maine – Act to Protect Privacy of Online Consumer Information
- Nevada – SB228
- New York – SHIELD Act
- Colorado – SB330
- Virginia – COPA
- Brazil – LGPD
- Singapore – PDPA
- China – PIPL
- South Korea – PDPA
- South Korea – PIPA
- Switzerland – DSD

Proposed Legislation/Talk Force Establishment

- Alabama – Consumer Privacy Act (DRAFT)
- Alaska – Consumer Data Privacy Act (DRAFT)
- Arizona – HB2883 (DRAFT)
- Connecticut – SB653 (DRAFT)
- Florida – Privacy Protection Act (DRAFT)
- Illinois – Consumer Privacy Act (DRAFT)
- Indiana – HB1363
- Kentucky – HB638 (DRAFT)
- Maryland – Online Consumer Protection Act (DRAFT)
- Massachusetts – Information Privacy Act
- Minnesota – Consumer Data Privacy Act
- Mississippi – Consumer Privacy Act (DRAFT)
- New York – Privacy Act/Digital Privacy Act
- North Carolina – Consumer Privacy Act
- North Dakota – HB1330 (DRAFT)
- Ohio – Personal Privacy Act
- Oklahoma – Computer Data Privacy Act (DRAFT)
- Pennsylvania – HB1326
- Texas – HB3743 (DRAFT)
- Utah – Consumer Privacy Act (DRAFT)
- Washington – Peoples Privacy Act
- West Virginia – HB2139 (DRAFT)
- Major U.S. Federal Proposals:
 - i. FTC Privacy Rulemaking (FTC)
 - ii. Protecting Consumer Information Act (S. 104)
 - iii. Information Transparency & Personal Data Control Act (S. 868)
 - iv. Data and Consumer Privacy Act (S. 104)
 - v. Consumer Data Privacy and Security Act (S. 104)
 - vi. Data Protection Act (S. 104)
- Australia – Privacy Act (Review)
- Canada – Digital Charter Implementation Act (DRAFT)
- China – PIPL
- India – DPDP



iaitam.org | Peace, Love & Asset Management | ACE 2022



8

Internet of Things



The diagram illustrates the Internet of Things (IoT) ecosystem. At the center is a cloud labeled 'IoT'. Surrounding it are various devices: a Nest Thermostat, an Amazon Echo, a Ring Doorbell, Wearables, and Appliances. Arrows connect these devices to the central IoT cloud, indicating their connectivity.



iaitam.org | Peace, Love & Asset Management | ACE 2022



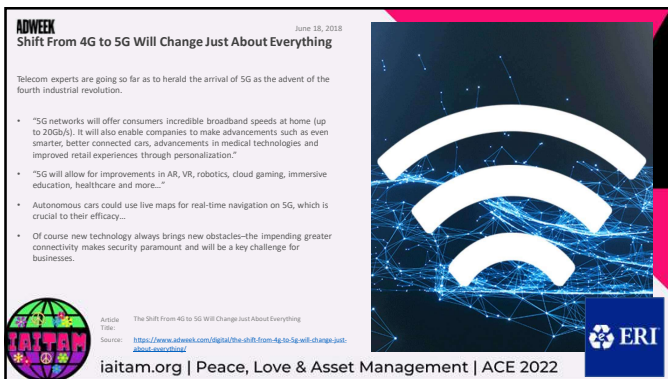
9



10



11



12

THE VERGE
Facebook's \$5 Billion Settlement with the FTC

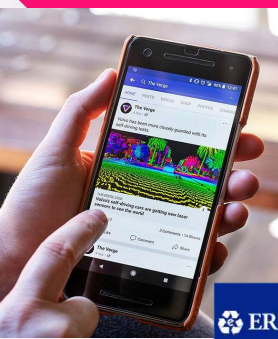

July 12, 2019

Facebook has reportedly reached a settlement with the Federal Trade Commission over repeated privacy violations, The Wall Street Journal reports. The FTC voted this week to approve a \$5 billion settlement, which has now moved to the Justice Department's civil division for review. It is unclear how long the review will take.

- In April, Facebook said it had set aside \$3 billion as part of an expected FTC fine. The settlement is expected to relate primarily to the 2018 Cambridge Analytica data privacy scandal.
- In its most recent quarterly earnings report, Facebook reported \$15.1 billion in sales, 26 percent ahead of the previous year. At the time, \$3 billion represented about 6 percent of the cash and marketable securities Facebook had on hand.
- Assuming the settlement is approved, the fine would be the largest in the history of the FTC. (The current record is a \$22.5 million fine against Google from 2012.)

Article Title: Facebook reportedly reaches \$5 billion settlement with the Federal Trade Commission
Source: <https://www.theverge.com/2019/7/12/2009253/facebook-ftc-settlement-fine-5-billion-justice-department>

iaitam.org | Peace, Love & Asset Management | ACE 2022

13

FS-ISAC
There is a C in ESG



November 1, 2020

Cyber is considered part of ESG (environmental, social, and governance) considerations; primarily within the governance aspect in terms of operational risk management, but also the social realm in terms of how communications are handled in the wake of an attack.

- In our recent ESG analysis of large and small banks in the US and Canada, governance tended to be the major ESG factor affecting credit risk, including both how companies manage cyber risk proactively and how they handle cyber incidents after they occur.
- Cyber risk now spans across all ESG considerations; it is directly related to financial risk as well as business position. As we have seen in 2020, it may spill over following environmental or natural disasters or pandemics.
- Successful attacks may impact capital, cash flow, earnings, and liquidity, but even more importantly, competitive position and customer confidence. Conversely, robust cyber risk management is a competitive advantage and will become a differentiating factor in a more digitally engaged world.

Article Title: There is a C in ESG
Source: <https://www.fs-isac.com/insight/there-is-a-c-in-esg>

iaitam.org | Peace, Love & Asset Management | ACE 2022

14

CNBC
Unstoppable Trends – From Green Energy to Cybersecurity



June 10, 2021

From green energy to equal access to education and technology, investors can find opportunities to make money through these "unstoppable trends," says Citi.

- David Ballin, chief investment officer at Citi Global Wealth, said that over the next five to 10 years, investors — especially younger ones — will place an "enormous emphasis" on sustainable and responsible investing, and not just focus on profits. "They will look at how companies treat the environment, employees, and even politics will form part of their investment decision..."
- He said the most important will be the "unstoppable trends" like climate change and social justice, including providing equal access to education and technology.
- Cybersecurity as part of ESG consideration: The ability for companies to deal with cybersecurity risks is also part of the whole ESG discussion, Ballin said.

Article Title: From green energy to cybersecurity, Citi names 'unstoppable trends' that investors can jump on
Source: <https://www.cnbc.com/2021/06/11/citi-on-esg-investments-green-energy-renewable-cybersecurity.html>

iaitam.org | Peace, Love & Asset Management | ACE 2022

15

Forbes
France Slaps Google With €50M GDPR Fine
 January 21, 2019

French regulators hit Google with a €50 million (about \$57 million) fine for violating European data protection and privacy rules.

- France's data privacy watchdog CNIL accused the search giant for lack of transparency, providing inadequate information and lack of valid consent regarding personalization of ads.
- The organization listed several alleged violations. Mainly, that the essential information about privacy that Google provides to users is not easily accessible. Google does not spell out why it is using personal data, how long the data stored, or what categories of data uses for ad-targeting, said CNIL.
- The fine is a blip. Google posted total revenue of \$111 billion for fiscal 2017, a figure seen rising to about \$137 billion for 2018.

Article Title: France Slaps Google With €50M Fine For Privacy Violation Under GDPR
 Source: <https://www.forbes.com/sites/jagadev/2019/01/21/france-slaps-google-with-50m-fine-for-privacy-violation-under-gdpr/>

“People expect high standards of transparency and control from us. We're deeply committed to meeting those expectations and the consent requirements of the GDPR.”
 — Google

ERL

aitam.org | Peace, Love & Asset Management | ACE 2022

16

BARCLAYS SECURITY
Marriott Hit With \$24 Million GDPR Privacy Fine Over Breach
 November 2, 2020

Hotel giant Marriott has been hit with the second largest privacy fine in British history, after it failed to contain a massive, long-running data breach.

- The fine, for violating the EU's General Data Protection Regulation, centers on a massive data breach involving the Starwood guest reservation system. The breach began with an attack against Starwood Hotels and Resorts Worldwide in July 2014.
- Exposed data included names, mailing addresses, phone numbers, email addresses, passport numbers and, in some cases, encrypted payment card information. The ICO says the identity of the attacker remains unknown.
- Marriott estimates that the breach exposed personal information for approximately 339 million customers worldwide, but cannot give a more precise number, as there may have been multiple records for individual customers.

Article Title: Marriott Hit With \$24 Million GDPR Privacy Fine Over Breach
 Source: <https://www.barclayssecurity.com/marriott-hit-24-million-gdpr-privacy-fine-over-breach-25388>

ERL

aitam.org | Peace, Love & Asset Management | ACE 2022

17

WSJ CYBERSECURITY
OCC Assesses \$60 Million Civil Money Penalty Against Morgan Stanley
 October 16, 2020

Federal regulators have fined two business units of Morgan Stanley \$60 million for data-security incidents that happened in 2016 and 2019.

- The Office of the Comptroller of the Currency, which regulates Morgan Stanley Bank NA and Morgan Stanley Private Bank NA, announced the penalty on Oct. 8. In both cases, sensitive information may have been left on decommissioned hardware.
- The data at risk may include Social Security numbers, asset value and holdings information, contact information and passport numbers, the bank said in July letters sent to customers and data attorneys general.
- The OCC alleges the bank failed to undertake proper due diligence on its vendors and monitor them, to assess the risks involved with decommissioning its hardware, and to keep an appropriate inventory of the data stored on the devices. These failings led to breaches of OCC rules on information security...

Article Title: OCC Fines Morgan Stanley Units For Data Security Incidents
 Source: <https://www.wsj.com/articles/occ-fines-morgan-stanley-units-for-data-security-incidents-11603384002>

ERL

aitam.org | Peace, Love & Asset Management | ACE 2022


18

WIRED
100 Million More IoT Devices Are Exposed—and They Won't Be the Last


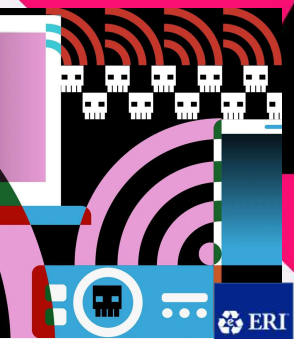
April 13, 2021

Over the last few years, researchers have found a shocking number of vulnerabilities in seemingly basic code that underpins how devices communicate with the internet. Now a new set of nine such vulnerabilities are exposing an estimated 100 million devices worldwide...

- All of the vulnerabilities, discovered by researchers at the security firms Forescout and JSDF, now have patches available, but that doesn't necessarily translate to fixes in actual devices, which often run older software versions.
- The researchers haven't seen evidence yet that attackers are actively exploiting these types of vulnerabilities in the wild. But with hundreds of millions—perhaps billions—of devices potentially impacted across numerous different findings, the exposure is significant.
- When it comes to long-term solutions, there's no quick fix given all the vendors, manufacturers, and developers who have a hand in these supply chains and products. But Forescout has released an open source script that network managers can use to identify potentially vulnerable IoT devices and servers in their environments.



Article Title: 100 Million More IoT Devices Are Exposed—and They Won't Be the Last
Source: <https://www.wired.com/story/homehack-iot-vulnerabilities-100m-millions-devices/>



aitam.org | Peace, Love & Asset Management | ACE 2022


19

Entrepreneur
A Casino Gets Hacked Through a Fish-Tank Thermometer



April 14, 2021

Secure your laptop. Secure your smart phone. Secure your tablet. And, before I forget, secure your fish tank. Yes, you heard me. Your fish tank.

- "The attackers used that (a fish-tank thermometer) to get a foothold in the network," she recounted. "They then found the high-roller database and then pulled that back across the network, out the thermostat, and up to the cloud."
- Connected devices are helping us track the status of deliveries, the hydration of golf courses and the optimal flow of water through pumping stations. And yes, even the temperature of fish tanks in a casino.
- These objects are being equipped with sensors and then connected back to networks, databases and communication systems. So much so that by 2025 some analysts predict that there will be as many as 31 billion connected devices worldwide.



Article Title: A Casino Gets Hacked Through a Fish-Tank Thermometer
Source: <https://www.entrepreneur.com/article/36843>



aitam.org | Peace, Love & Asset Management | ACE 2022


20

tom's guide
3.3 Million Customers Hit by VW Data Breach



June 11, 2021

Volkswagen Group of America announced that more than 3.3 million potential and actual Audi customers in the U.S. and Canada had personal data exposed. At least some data was taken without authorization.

- "A third party obtained limited personal information" from an unnamed sales and marketing vendor, a letter sent to state attorneys general and obtained by TechCrunch said. Further investigation revealed that the vendor had "left electronic data unsecured at some point between August 2019 and May 2021."
- The data stolen from Volkswagen Group of America appears to be up for sale in a cybercrime marketplace, reports Vice Motherboard. The data for sale includes names, email addresses, mailing addresses, telephone numbers and Vehicle Identification Numbers, Vice says the seller stated.
- The implication is that the unauthorized party got hold of only the least sensitive data, which would not normally raise red flags. But because of the highly sensitive nature of some of the other exposed data, Volkswagen is providing free identity-theft-protection for 900,000 affected persons.



Article Title: 3.3 million customers hit by VW data breach — what to do
Source: <https://www.tomsguide.com/news/vw-audi-data-leak>





aitam.org | Peace, Love & Asset Management | ACE 2022

21

S&P Global
Cybersecurity: A Growing ESG Concern
May 25, 2021

To facilitate long term, sustainable growth, it is imperative to analyze the environmental, social and governance (ESG) performance of companies and examine how activity in the markets influences the world in which we live.

- The cyber insurance market is underdeveloped, and cyber cover is often tacked onto existing liability or property insurance policies that were not originally intended to cover cyber risk.
- The cyberattack on Colonial Pipeline is the most recent incident to raise questions over whether industries are adequately prepared to mitigate risk and safeguard vulnerabilities.
- To effectively and efficiently protect assets from cyberattacks, companies need to go beyond IT security and evaluate cyber risk from cyber-informed engineering perspectives.



 Article Title: Cybersecurity: A Growing ESG Concern
Source: <https://www.spglobal.com/en/research-insights/features/may-2021-cyber-security>
iaitam.org | Peace, Love & Asset Management | ACE 2022 

22

Forbes
U.S. Defense Electronics Supply Chain Dangerously Thin And Falling Behind
June 30, 2021

The U.S. is facing shortages and security vulnerabilities with printed circuit boards and integrated circuit substrates crucial to the sexiest weapons systems we have.

- Over the last year, the global semiconductor shortage has received manifold attention but the broader U.S. electronics supply chain has been almost completely ignored.
- Farming out electronics manufacturing has yielded a lack of capacity, unreliable materials sourcing, the twin dangers of defense electronics hardware hacking and sabotage by U.S. adversaries, and led to a failure to keep pace technologically. These were avoidable dangers.
- The PCBetter Act, introduced in April by Sen. Josh Hawley, R-Mo., would require defense contractors to tell the Pentagon if China, Russia, Iran and North Korea made any of the printed circuit boards in systems they were supplying. Hawley noted that "Chinese printed circuit boards pose a serious threat to the integrity of America's defense systems."



 Article Title: America's Defense Electronics Supply Chain Is Dangerously Thin And Falling Behind
Source: <https://www.forbes.com/sites/ericlougher/2021/06/30/americas-defense-electronics-supply-chain-is-dangerously-thin-and-falling-behind/>
iaitam.org | Peace, Love & Asset Management | ACE 2022 

23

Bloomberg
Amazon Gets Record \$888 Million EU Fine Over Data Violations
July 30, 2021

Amazon.com Inc. faces the biggest ever European Union privacy fine after its lead privacy watchdog hit it with a 745 million-euro (\$888 million) penalty for violating the bloc's tough data protection rules.

- CNPD, the Luxembourg data protection authority slapped Amazon with the record fine in a July 16 decision that accused the online retailer of processing personal data in violation of the EU's General Data Protection Regulation, or GDPR.
- "It's a first step to see a fine that's dissuasive, but we need to remain vigilant and see if the decision also includes an injunction to correct the infringing behavior," said Bastien Le Querrec, a member of La Quadrature's litigation team...
- The privacy probe also adds to intense antitrust scrutiny of Amazon's business in Europe. Amazon is being probed by the EU over its use of data from sellers on its platform and whether it unfairly favors its own products.

 Article Title: Amazon Gets Record \$888 Million EU Fine Over Data Violations
Source: <https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach>
iaitam.org | Peace, Love & Asset Management | ACE 2022 



24

BBC
The Lost Tablet and the Secret Documents
August 11, 2021

The BBC has gained exclusive access to an electronic tablet left behind on a battlefield in Libya by a Wagner fighter, giving an unprecedented insight into how these operatives work.

- "... a Samsung tablet had been retrieved from a battlefield in western Libya." Russian mercenaries had been fighting there in support of Libyan renegade general Khalifa Haftar, against the UN-backed Government of National Accord (GNA). It's believed the tablet had been left behind when the fighters retreated in the spring of 2020.
- Remarkably, the information on it was easy to access. I discovered dozens of files - ranging from manuals for anti-personnel mines and improvised explosive devices (IEDs), to reconnaissance drone footage... But it was a maps app that stood out - layers of military maps of the front line, all marked in Russian.
- The Wagner group is one of the most secretive organisations in Russia. Officially, it doesn't exist - serving as a mercenary is against Russian and international law. But up to 10,000 operatives are believed to have taken at least one contract with Wagner over the past seven years.

Article Title: The lost tablet and the secret documents - Clues pointing to a shadow Russian army
Source: <https://www.bbc.co.uk/news/health-58162626/the-lost-tablet-and-the-secret-documents>

 **iataam.org | Peace, Love & Asset Management | ACE 2022** 



25

HEALTH SECURITY
Improper Hard Drive Disposal Leads to Health Data Breach for 100K
September 21, 2021

Over 100K patients at HealthReach Community Health Centers in Maine may have had their personal data leaked due to improper disposal of the health center's hard drives.

- The hard drives were improperly disposed of by an employee at a third-party data storage facility, according to a statement shared with the Maine attorney general's office.
- The incident occurred on April 7 and HealthReach discovered the breach on May 7. Further investigation determined that some personally identifiable information (PII) and protected health information (PHI) of patients was involved.
- The information at risk includes names, addresses, birth dates, Social Security numbers, medical insurance information, lab results, medical record numbers, and treatment records.

Article Title: Improper Hard Drive Disposal Leads to Health Data Breach for 100K
Source: <https://healthsecurity.com/news/improper-hard-drive-disposal-leads-to-health-data-breach-for-100k>

 **iataam.org | Peace, Love & Asset Management | ACE 2022** 



26

BUSINESS JOURNAL
Zoom to Pay \$85M for Privacy Miscues at Start of Pandemic
August 2, 2021


Zoom will pay \$85 million to settle a lawsuit alleging that weak privacy controls opened too many peepholes into the personal information of users and that it was too easy for outsiders to disrupt video meetings during the early stages of the pandemic.

- The lawsuit alleged that the Silicon Valley company violated the trust of millions of people by sharing the personal information of users with platforms like Facebook, Google and Microsoft-owned LinkedIn.
- The case, which consolidated 14 different lawsuits filed since March 2020, also targeted the disruptive practice of "Zoombombing" — a term coined to describe hackers who broke into videoconferencing meetings being held by others.
- The payment amounts are expected to average \$34 or \$35 for those who subscribed to Zoom's paid version, and \$11 or \$12 for the overwhelming majority who used the free version, based on estimates in court documents.

Article Title: Zoom to pay \$85M for privacy miscues at start of pandemic
Source: <https://thebusinessjournal.com/zoom-to-pay-85m-for-privacy-miscues-at-start-of-pandemic/>

 **iataam.org | Peace, Love & Asset Management | ACE 2022** 

27





NY AG Notifies 17 Companies of Breaches – 1.1 Million Accounts Compromised


January 5, 2022

Seventeen companies have been informed of cyberattacks that compromised user information by New York Attorney General Letitia James following an investigation into credential stuffing.

- More than 1 million customer accounts were compromised due to the attacks, which James said were previously undetected. The 17 businesses affected include well-known online retailers, restaurant chains, and food delivery services.
- The FBI said last year that credential stuffing attacks – which involve repeated, automated attempts to access online accounts using usernames and passwords stolen from other online services – have been used to compromise 50,000 online bank accounts since 2017.
- After contacting the companies, all 17 investigated the OAG's findings and took steps to protect users. OAG said, "nearly" all of the companies "implemented, or made plans to implement additional safeguards."

Article Title: NY AG notifies 17 companies of breaches, says 1.1 million accounts compromised in attacks
Source: <https://www.aitam.com/article/ny-ag-notifies-17-companies-of-breaches-says-1-1-million-accounts-compromised-in-attacks/>

 **aitam.org | Peace, Love & Asset Management | ACE 2022** 



28



Currys' Smart TV Repair Raises Data Protection Issues

February 9, 2022

The case is likely to draw interest from recyclers of waste electrical and electronic equipment (WEEE), as concern over data on devices is often cited as a reason for people hoarding old electricals at home.

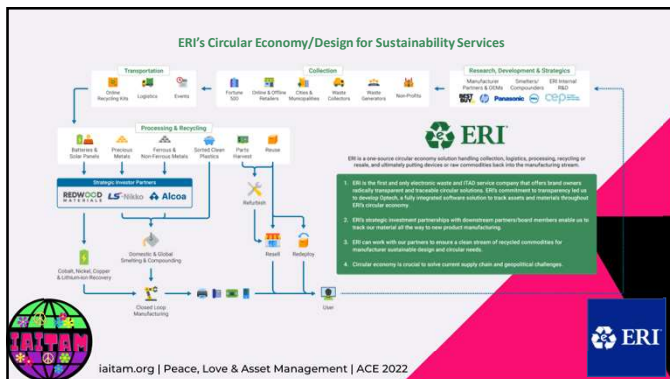
- Currys' technical staff determined that any repair of the television would be "disproportionately costly" and offered to write off the unit and compensate Mr. Stadler with a voucher. He accepted and used the voucher to buy a new television.
- Mr. Stadler's original Smart TV was sold on to a third party with the data not wiped, and someone used his Amazon Prime account to spend £3.49 on a film.
- Mr. Stadler brought a claim for £5,000 in damages against Currys Group Ltd before the High Court, on the basis that data protection laws were breached and that he suffered "psychological distress, anxiety, loss, and damage," among other reasons.

Article Title: Currys' Smart TV Repair Raises Data Protection Issues
Source: <https://www.aitam.com/news/currys-smart-tv-repair-raises-data-protection-issues>

 **aitam.org | Peace, Love & Asset Management | ACE 2022** 



29



30



SOC 2 Certified

ERI Is First ITAD and Electronic Waste Recycler in the World to Earn SOC 2 Certification

SOC 2 is a globally-recognized data security and controls certification, awarded following a rigorous audit.

ERI's certification verifies that our practices, policies, procedures and operations all meet the SOC 2 standards for security and data protection.

SOC 2 Certification Confirms:	SOC 2 Certification Benefits ERI Customers By:
ERI has proper protocols in place for network security & intrusion detection.	Automating the audit process. Many Fortune 500 companies allow for SOC 2 certification in place of laborious audits and paperwork when onboarding a partner like ERI and when conducting annual audits.
ERI properly monitors performance, encryption, and access controls while maintaining strict disaster recovery and incident handling protocols.	Demonstrating ERI's commitment to security and data protection at the highest level.
ERI has a stringent quality assurance and process monitoring in place to maximize security.	Adding another competitive advantage for ERI, which is already an industry leader with existing certifications such as NAAD, e-Stewards, and R2. No other ITAD or e-waste provider is certified by these bodies plus SOC 2.





iaitam.org | Peace, Love & Asset Management | ACE 2022

31



People. Planet. Privacy.™



Contact Information



John Shegerian
Co-Founder and Chairman/CEO

jss@eridirect.com
(559) 974-8588



iaitam.org | Peace, Love & Asset Management | ACE 2022

32
