AI on the Edge: Legal Considerations for Artificial Intelligence Systems from Peripheral Devices

Second Annual AI Legal Summit Hosted by Robins Kaplan LLP and the Berkeley Center for Law & Technology | May 12, 2021

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

PRESENTERS

Kevin M. Pasquinelli

Partner
Robins Kaplan LLP
KPasquinelli@RobinsKaplan.com

Deepak Dutt

CEO
Zighra
Deepak@Zighra.com

Michael D. Reif

Partner
Robins Kaplan LLP
MReif@RobinsKaplan.com

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

AGENDA

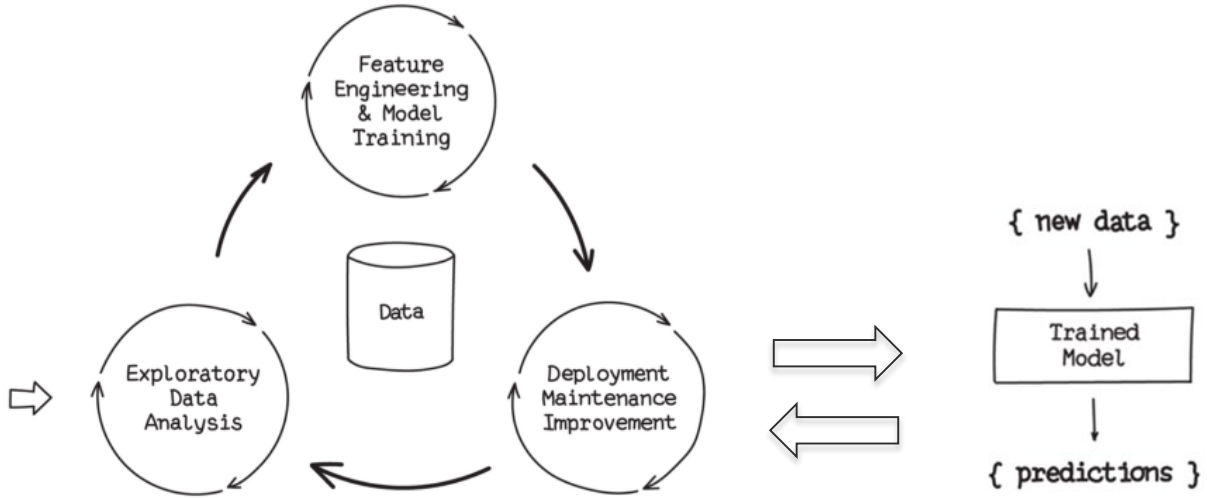
- What is Edge AI and why it's important
- How patentable is Edge AI?
- Increased security risks: what constitutes "reasonable security" in an Edge AI environment?
- Zighra: Biometric Authentication & Security in an Edge AI environment
- Increased privacy risk: what additional privacy precautions should be taken in an Edge AI environment?
- Open Panel – Q & A

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

Traditional AI Is Cloud Bound

Figure source: Toward Data Science



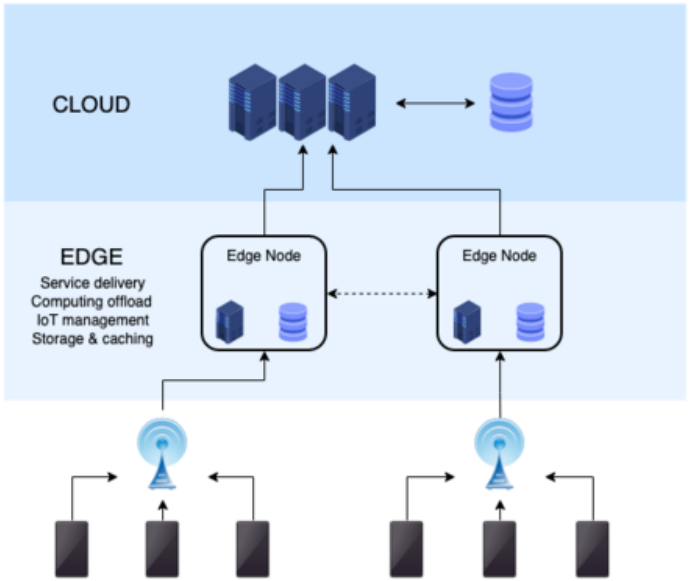
Cloud

Cloud or Edge

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

Edge Computing Paradigm



Features

- Intermediate computing layer
- Does not replace cloud or data center.
- Offloads cloud processing and enables quicker response for edge nodes

Benefits

- Reduced Latency
- Reduced Bandwidth
- Complete or Limited Autonomy
- Increased or Reduced Security / Privacy?

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

AI on the Edge Places Intelligence in the Edge Computing or Edge Node

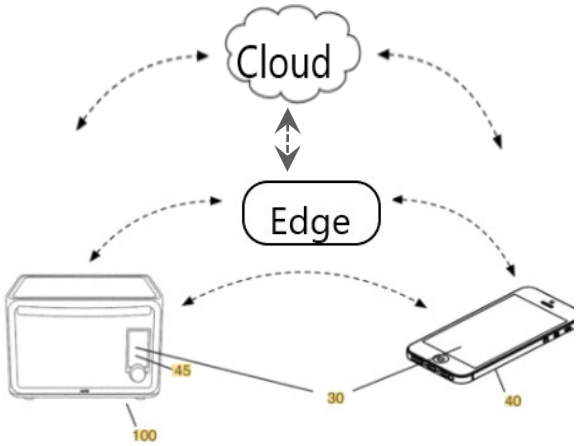


FIGURE 4

Intelligent Oven

Examples

- Intelligent Appliances
- Autonomous Drones & Vehicles
- Video Analytics (security)
- Smart Phone face recognition
- Robots (Stock Room, Manufacturing Floor)

Risks & Opportunities

- The number of potentially insecure data transfers.
- Increasing Amount of Data Collected & Stored on Edge
- Increased physical availability
- Increased local processing

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

Edge AI: Patent Eligibility May Be Higher Than Traditional AI

- **U.S. Latest Results**
  - 2019 Patent Eligibility Guidance Still Governs
  - No informative litigation on “real” AI.
  - Allowance and 101 Rejections vary widely across art units
  - Practical Applications of AI improving the prior art remain strongest (e.g. image analysis)
- **European Guidance**
  - Applications of AI/ML are patent eligible for a technical contribution
  - The algorithm must be causally linked to the technical effect.
  - Example: Neural Network in a Heart-monitoring apparatus for the purpose of identifying irregular heartbeats.

https://www.ipwatchdog.com/2020/10/25/determining-likelihood-ai-patent-application-will-allowed-uspto/id=126687/
https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_3_1.htm EPO Patent eligibility guidance

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

What Constitutes "Reasonable Security" in an Edge AI Environment?

- California CCPA and CRA (9th Cir.)
- Federal Trade Commission
- CA Attorney General

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

CCPA & CRA Related Cases Helps Establish What Is Not Necessarily Unreasonable

- Alleging that reasonable security was not taken is insufficient *See Razuki v. Caliber Home Loans, Inc.*, 2018 WL 6018361, at *1 (S.D. Cal. November 15, 2018) (dismissing § 1798.81.5 claim)
- Awareness of higher quality security protocols than the ones taken is not necessarily a lack of reasonable security. *See Razuki v. Caliber Home Loans, Inc.*, 2018 WL 6018361, at *1 (S.D. Cal. November 15, 2018) (dismissing § 1798.81.5 claim)
- A security breach alone does not mean that reasonable security was not taken *See Anderson v. Kimpton Hotel & Restaurant Group, LLC*, Cas No. 19-cv-01860-MMC, 2019 WL 3753308 (N.D. Cal. Aug. 8, 2019)

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

CCPA & CRA Related Cases Helps Establish What Could be Unreasonable (Continued)

- If proven as true the following could amount to a lack of reasonable security: *See Adobe Sys., Inc*. 66 F.Supp. 3d 1197 (N.D. Cal. 2014)
  - (1) Lack of conformance to industry standards
  - (2) Poor encryption and storage of passwords
  - (3) Poor intrusion detection
  - (4) Improperly segmenting its network
  - (5) Insufficient network level system controls
- Failure to encrypt customer's data could amount to a lack of reasonable security. *See DugasStarwood Hotels & Resorts Worlwide, Inc.* Case No. 3:16-cv-00014-GPC-BLM, 2016 WL 6523428 (S.D. Cal Nov. 3 2016); *See also In re Sony Gaming Networks*, 996 F.Supp. 2d 942, 966 (S.D. Cal. 2014)

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

FTC: “Reasonable & Appropriate Security”

- Require secure passwords and authentication
- Store sensitive personal information securely and protect it during transmission
- Segment your network and monitor
- Secure remote access & ensure endpoint security

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

CA Attorney General Suggests a Heightened Cybersecurity Standard of Care

- Center for Internet Security's Critical Security Controls identify a minimum level of information security→ lack thereof constitutes a lack of reasonable security.
- Multi-factor authentication available on consumer-facing on-line accounts that contain sensitive personal information.
- Strong encryption to protect personal information

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

Preventative Reasonable Security Guidelines in Edge AI

- Consider the nature and scope of the product and the sensitivity of the personal information being collected
- Adhere to Industry Standards where appropriate
- Use security from providers
- Strong authentication methods
- Encrypted & Secure transmission
- Segmentation and endpoint protection
- Encrypted local storage

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

Voir plus bas pour la version française de ce message.

MGM RESORTS INTERNATIONAL

Dear Guest,

We are writing to notify you of an issue that involves your personal information. On July 10, 2019, we learned that an unauthorized party had accessed and downloaded certain MGM Resorts guest data from an external cloud server a few days earlier. The affected information may have included names, contact information (such as postal addresses, email addresses, and phone numbers), and dates of birth. The specific data affected differed for each impacted individual.

Promptly after learning of the issue, we took steps to enhance our security measures such as by further strengthening our monitoring capabilities to detect unauthorized system activity. We engaged a leading third-party data security expert to assist with our investigation of the incident and coordinated with law enforcement authorities.

We recently identified that your information was affected by this issue. We take our obligation to safeguard personal information very seriously and are alerting you so you can take steps to help protect against the risk of misuse of your information. We are providing you with credit monitoring services for one year at no cost to you, and encourage you to follow the instructions below to enroll in these services.

We hope this information is useful to you. If you have any questions regarding this issue, please contact 1 (888) 261-9692 from 9:00 am - 5:00 pm, Eastern Time. We regret any inconvenience this may cause you.

Sincerely,

MGM Resorts International

MGM

Full names

Emails/Phone #

Addresses

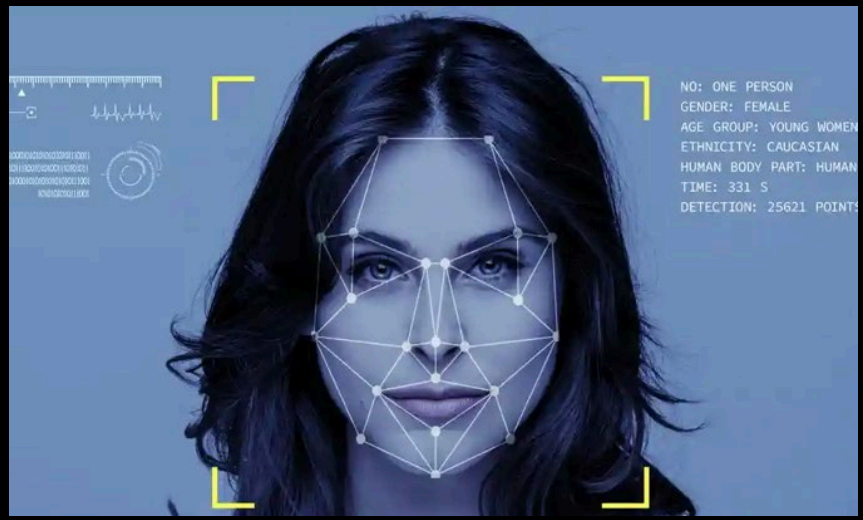
DoB

Twitter Blames Mobile Carrier for Dorsey’s Account Hack

Twitter

Fingerprints, facial recognition and other PII discovered on publicly accessible database

Suprema

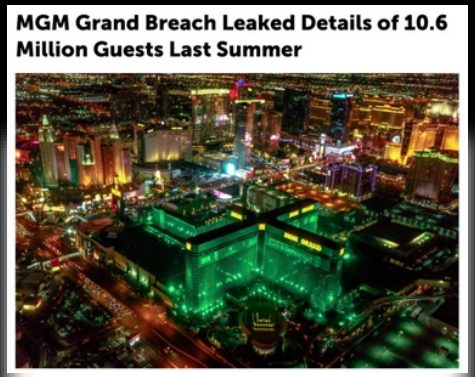


Problem

* fundamental issue - Centralized Architectures

* U.S. Breaches Cost Over $1.8 Trillion in 2019

Personal Info Breach

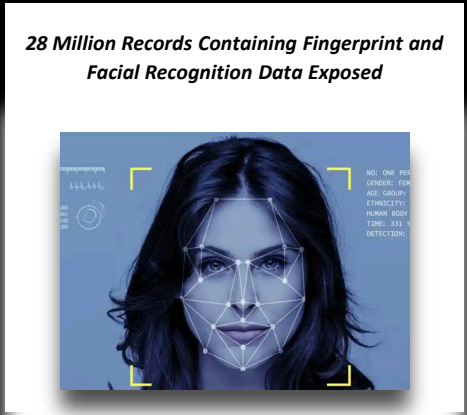


Privacy

SIM Swap Fraud

Security

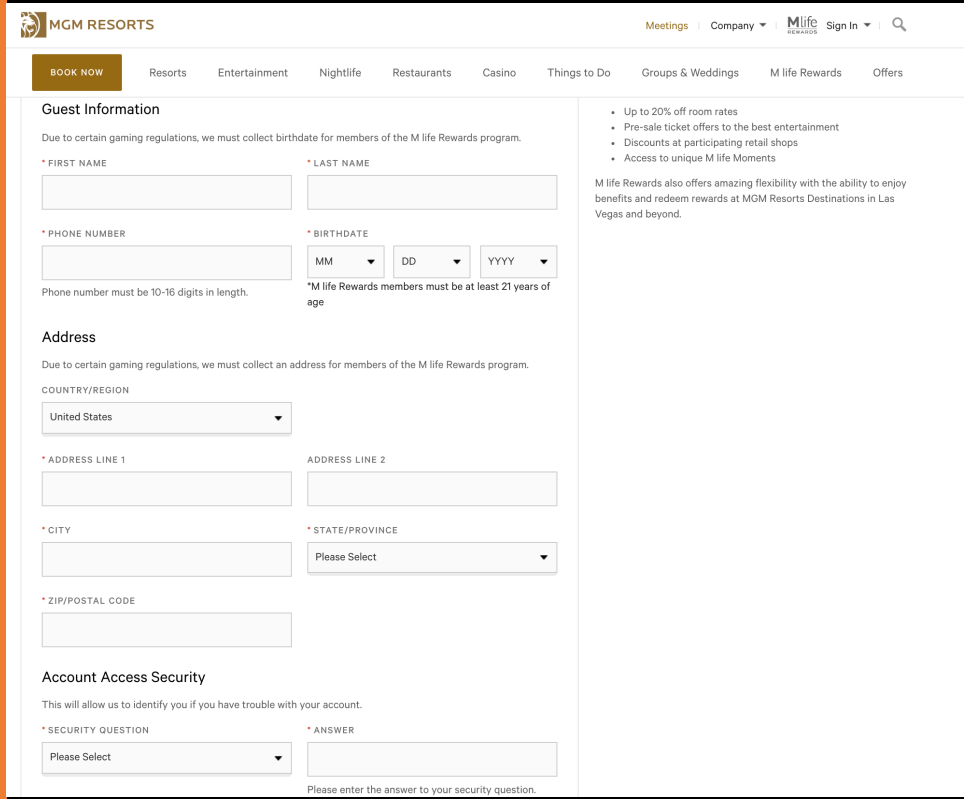
Biometric Breach



Identity

Privacy

- Full name
- Home address
- Email
- Phone number
- Dates of birth
- Drivers license/Passport Info



Security

- Email
- Social Media
- Bank Accounts
- Crypto Accounts

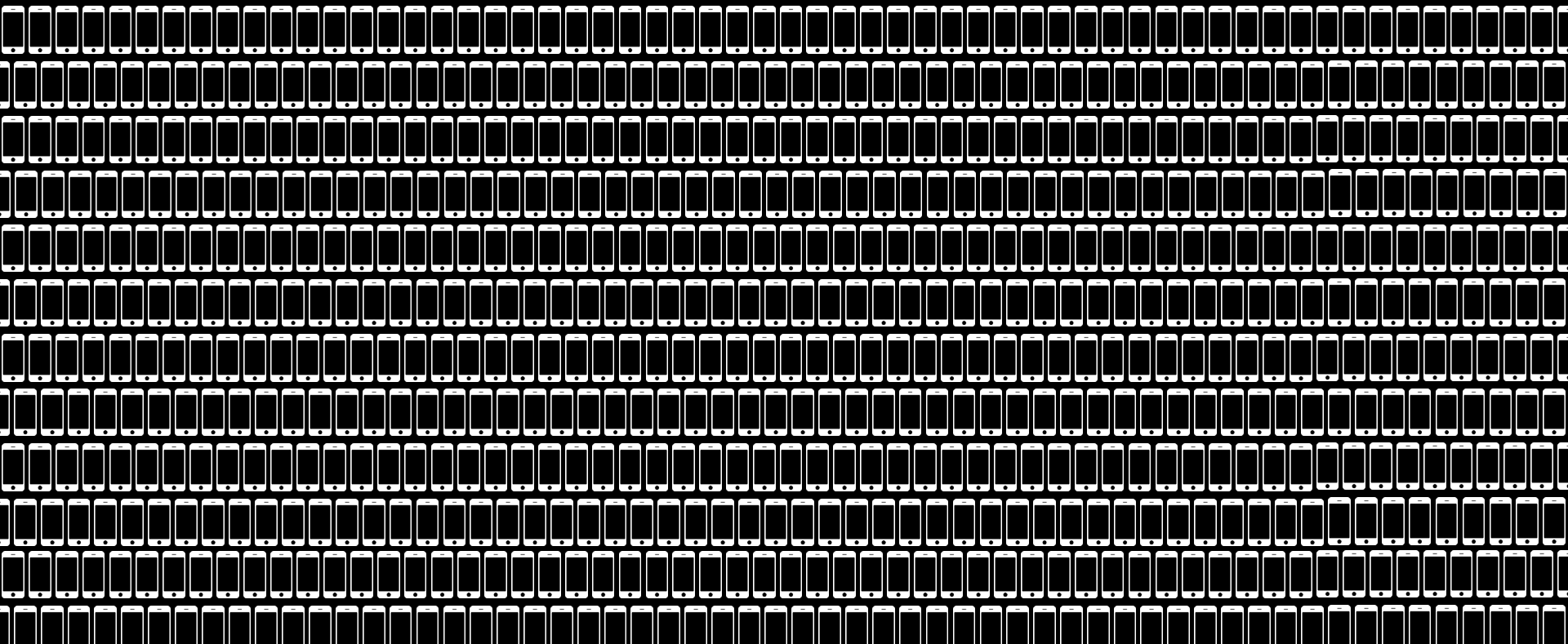
Identity

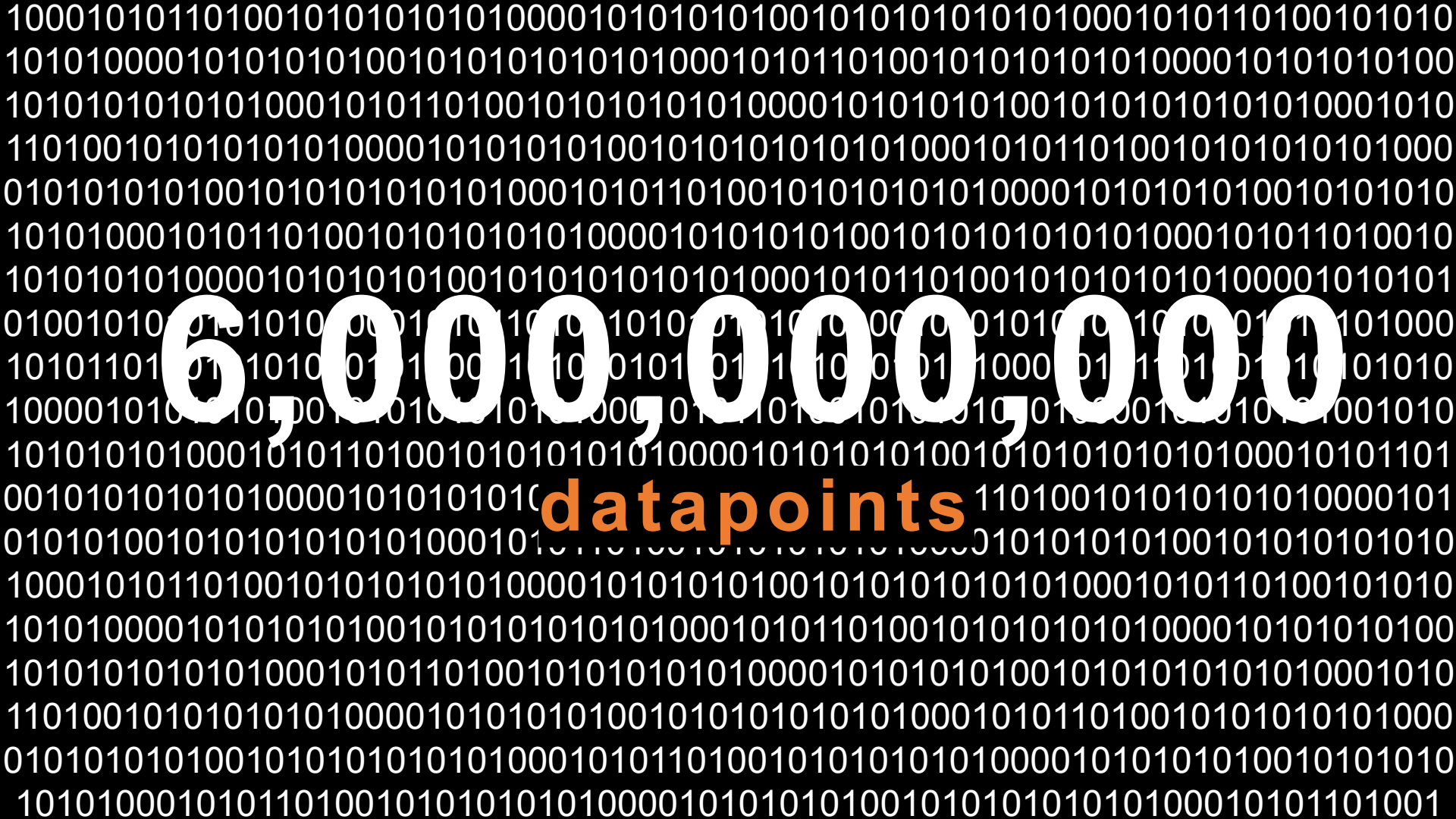
- Synthetic ID
- Medical ID
- Financial ID
- Tax ID

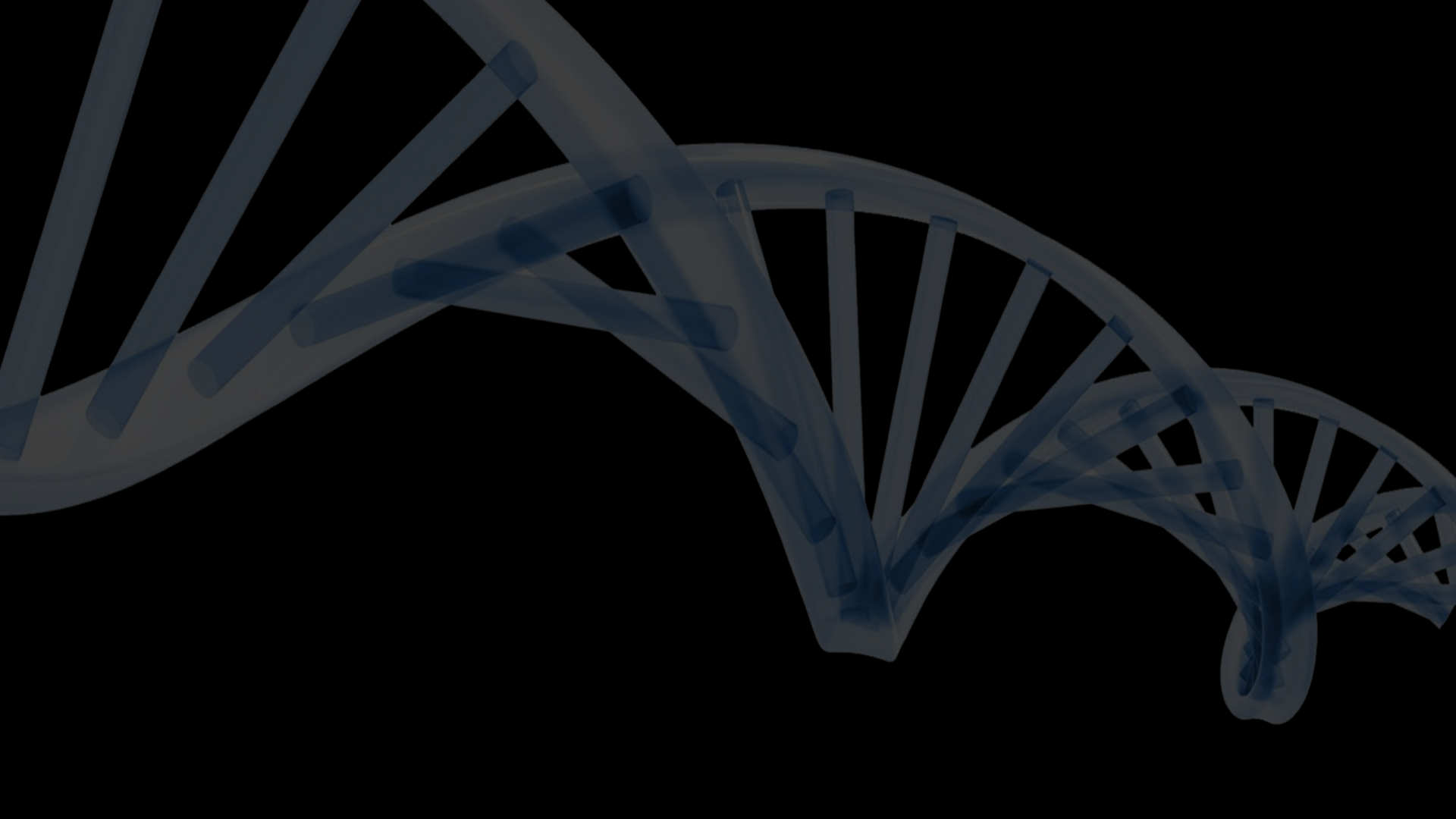
Decentralized Trust

70 countries

700 device types




6,000,000,000
datapoints

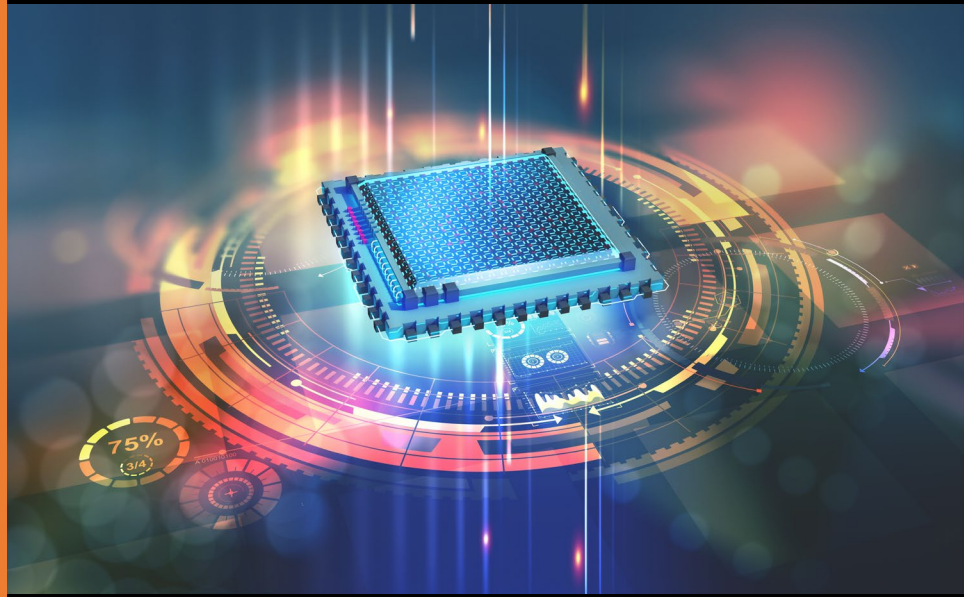


Privacy – On-device Processing

- Personal data stays on device.
- Protects behavioral data from compromise.
- Enable personalized services without compromising privacy.

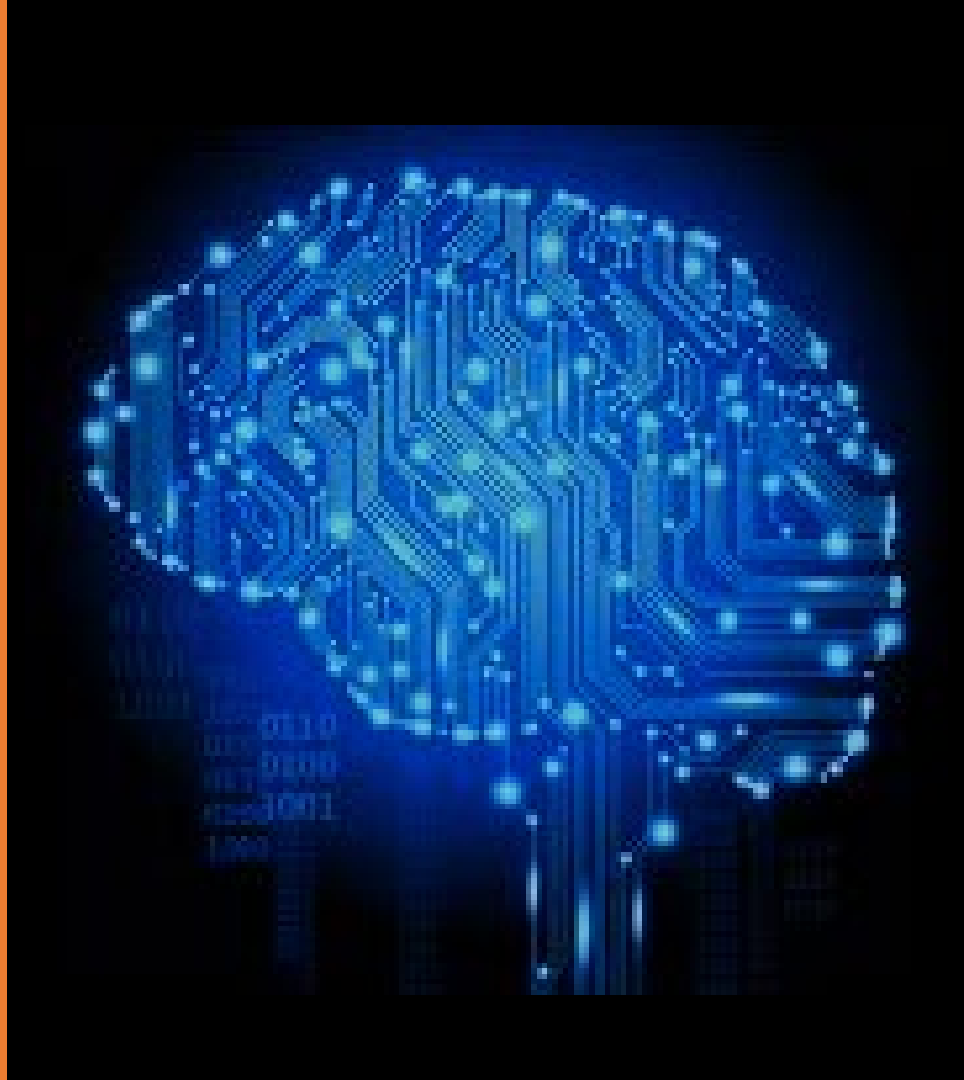
Security – Hardware-based Encryption

- H/W encryption of personal data.
- Cryptographic keys stay on device.
- Smartphone vendors releasing crypto specific chips.



Identity – Continuous Behavioral Authentication

- Monitors for suspicious activity on device.
- Detects anomalies in device-user interactions.
- Always on behavioral engine detects and blocks malware.

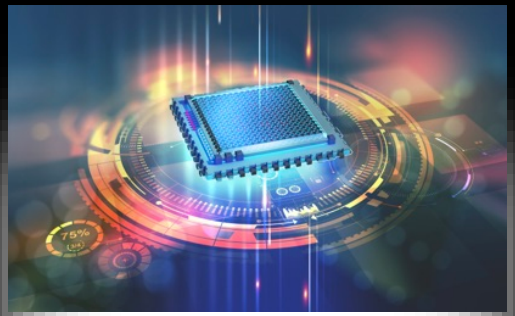


Solution - AI-Powered Continuous Authentication

On-device Processing

Privacy

H/W level Encryption



Security

Continuous ID Proofing

Identity


698.11
698.11
226.34
875.73

Privacy Considerations in an Edge AI Environment

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP

REWRITING THE ODDS

Duality of the Edge for Privacy and Security

- **Increased risks when moving processing away from a central source**
  - Data and privacy leakage
  - Data integrity
- **Increased opportunities to build privacy-by-design into the Edge**
  - Data localization
  - Reduced data transfer
  - Compartmentalization

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

Privacy laws: Wild West vs. shoehorning

- Regulatory vacuum for AI at the Edge
- Presents opportunity for creativity and innovation

- But, like nature, regulators abhor a vacuum
- That means trying to fit Edge into existing laws (and not always very neatly)

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

Existing laws to consider

GDPR

PIPEDA

CCPA

PIPL

BIPA

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS

Countermeasures

- Encryption
- Authentication
- Auditing
- System analysis
- Policy-based mechanisms
- Logging

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP

REWRITING THE ODDS

QUESTIONS?

Kevin M. Pasquinelli

Partner
Robins Kaplan LLP
KPasquinelli@RobinsKaplan.com

Deepak Dutt

CEO
Zighra
Deepak@Zighra.com

Michael D. Reif

Partner
Robins Kaplan LLP
MReif@RobinsKaplan.com

Berkeley Center for Law & Technology

ROBINS KAPLAN LLP
REWRITING THE ODDS