

OX-2025-0106

Customer Information

Opening Comments from
Missouri Office of the Public Counsel
Chief Economist, Geoff Marke

How we got here?

6 years, 5 months, and 27 days ago...

- June 19, 2018: Direct testimony filed (Case Nos. ER-2018-0145 and 0146) recommending that the Commission order a rule-making workshop to amend Chapter 13 billing rules to account for the substantive changes in billing, data practices, and associated privacy concerns.
- June 27, 2018: Staff files a motion to establish a rulemaking working case within the Commission's affiliate transaction rules on the treatment of customer information in Case No. AW-2018-0393
- July 11, 2018: Commission grants request

- Staff files rulemaking workshop request and draft rules (6/27/2018)
- August 24, 2018: The following parties filed comments:

- American Civil Liberties Union (“ACLU”)
- State Rep. Bill Kidd
- TGH Litigation LLC
- Missouri Attorney General Joshua D. Hawley
- Office of the Public Counsel
- Spire Missouri
- Missouri-American Water
- Ameren Missouri
- KCPL/GMO
- Liberty Utilities
- Consumer Council & Empower Missouri
- ArchCity Defenders, Inc.

- Workshop (10/9/2018)
- Response to Staff questions (11/30/2018)
- Staff drafts 2nd rule (9/16/2019)
- Response to Staff draft rules (12/9/2019)
- Staff 3rd draft of rules (2/18/2020)
- Two utilities file compliance costs (3/20/2020)
 - 4 years, 8 months, and 20 days later
- OX-2025-0106 opens (9/26/2024)

**What does the public think
about data privacy?**

KPMG

Bridging the Trust Chasm (2021)

- Lucas, O. et al. (2021) Bridging the trust chasm. *KPMG*. <https://cyberights.org/wp-content/uploads/2023/05/KPMG-Corporate-data-responsibility-bridging-the-consumer-trust-gap-PDF-CRO-Cyber-Rights-Organization.pdf>

- 86% of respondents say data privacy is a growing concern for them.
- 48% of respondents say they would be more comfortable with companies collecting and using their personal data if it was made fully anonymous.
- 40% of respondents say they would willingly share personal data if they knew exactly how it would be used and by whom.
- Yet only, 52% of business leaders say their company has taken active steps to demonstrate how consumer data will be used.

A shockingly low number of consumers can identify circumstances that would prompt them to willingly share their personal data.

Only 12 percent of the U.S. general population say they would share their data to make online ads more relevant to their interests, and only 17 percent say they would do it to help businesses create better products and services. Even to advance the greater good, only 30 percent say they would share their data.

As one survey respondent noted, "I don't feel comfortable with corporations having my personal information on file, as I am concerned about hacking and information leaks. Even if their intentions are good and legitimate, it leaves my information vulnerable." Another respondent added: "I don't want my information ever sold or shared with other companies. I also don't want my shopping behavior to be used to target me for other purchases."

KPMG concludes w/ 3 recommendations:

1. Be more explicit and transparent about how consumer data will be used
2. Give consumers more direct control over their personal data
3. Make data anonymous to whatever extent possible

Pew Research

How Americans View Data Privacy (2023)

McClain, C. et al., (2023) Views of data privacy risks, personal data and digital privacy laws. *Pew Research Center*. <https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306/>

Americans largely favor more regulation to protect personal information

Overall, 72% say there should be more government regulation of what companies can do with their customers' personal information. Just 7% say there should be less regulation. Another 18% say it should stay about the same.

- Only 21% of U.S. adults are confident that those with access to their personal information will do what is right.
- 81% of U.S. adults are concerned about how Companies use(s) the data they collect about them.
- 61% of users agree that privacy policies are ineffective at explaining how companies use their data.

Consumer Reports

American Experiences Survey

September 2024 Omnibus Results

- Medintz, S. (2024) Americans want much more online privacy protection than they're getting. *Consumer Reports*.
<https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306/>

- **Would you support or oppose a law that regulates how companies can collect, store, share, and use people's personal data?**
 - **78% of respondents would support a law regulating how companies can collect, store, share, and use personal data**
 - **81% of Democratic or Democratic-leaning would support such a law**
 - **79% of Republican and Republican-leaning would support such a law**

Which, if any, of these consumer protection topics are most interested in (choose up to three)?

| | |
|--|-----|
| Advocating for laws that would prevent companies from sharing people's personal data without their knowledge | 42% |
| Protecting food from contamination by bacteria, such as salmonella or e coli | 37% |
| Working towards ensuring the safe and ethical use of artificial intelligence | 30% |
| Protecting the environment from contamination by plastics | 30% |
| Protecting food from contamination by plastics | 27% |
| Protecting food from contamination from heavy metals | 26% |
| Identifying unsafe products or toys for kids | 20% |
| Advocating for safety regulations around self-driving cars | 12% |
| Advocating for regulation around banking apps | 8% |
| Some other consumer protection issue, please specify | 1% |
| I am not interested in consumer protection issues | 13% |

CISCO

2024 Data Privacy Benchmark Study

- CISCO (2024) Privacy as an Enabler of Customer Trust. *CISCO 2024 Data Privacy Benchmark Study*. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-privacy-benchmark-study-2024.pdf?CCID=cc000160&DTID=odicdc000016&OID=rptsc032067 /

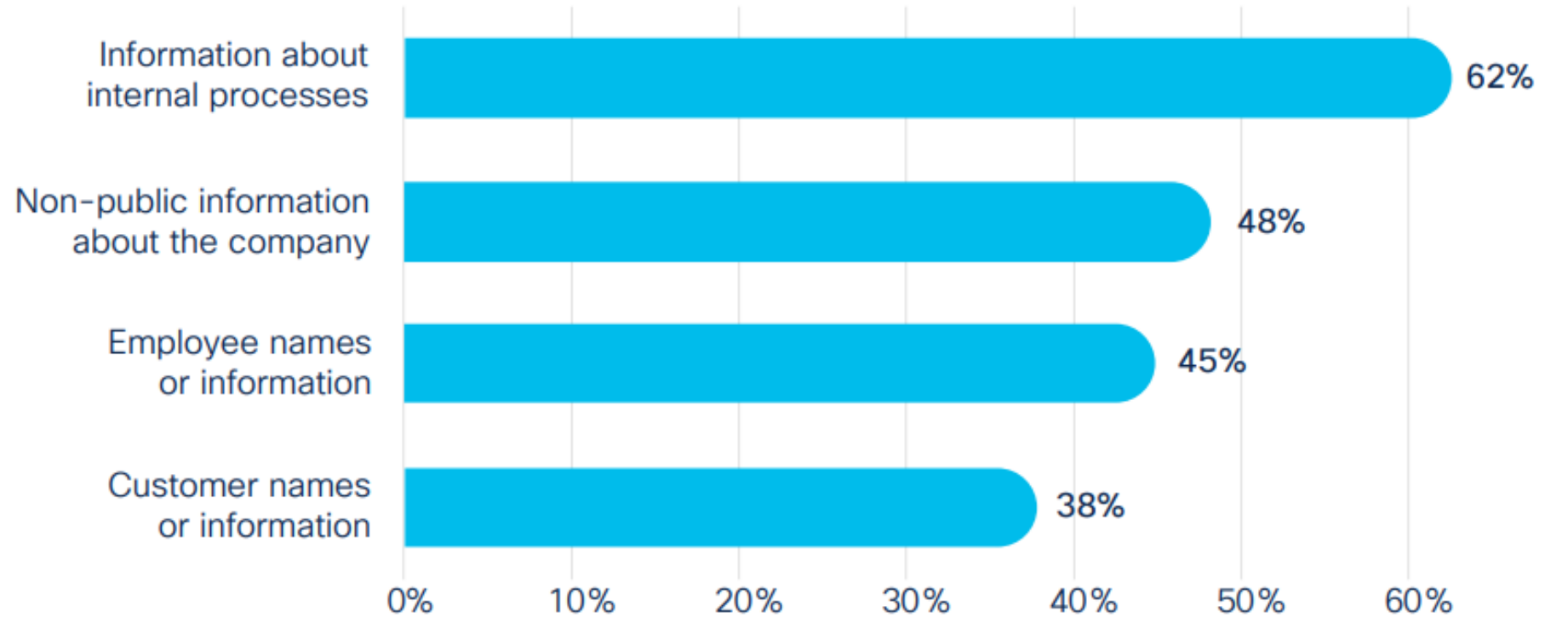


94%
of organizations say their
customers won't buy from them if
data is not properly protected



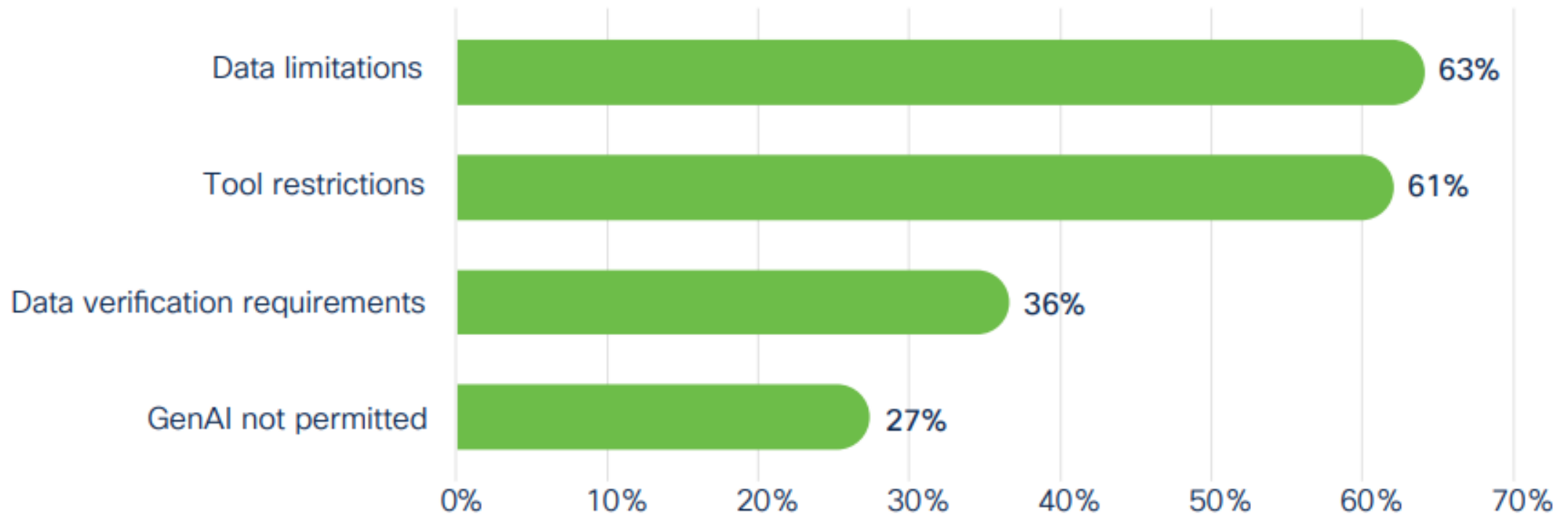
48%
are entering non-public information
about the company into GenAI
apps

Figure 18. Types of information entered into GenAI applications



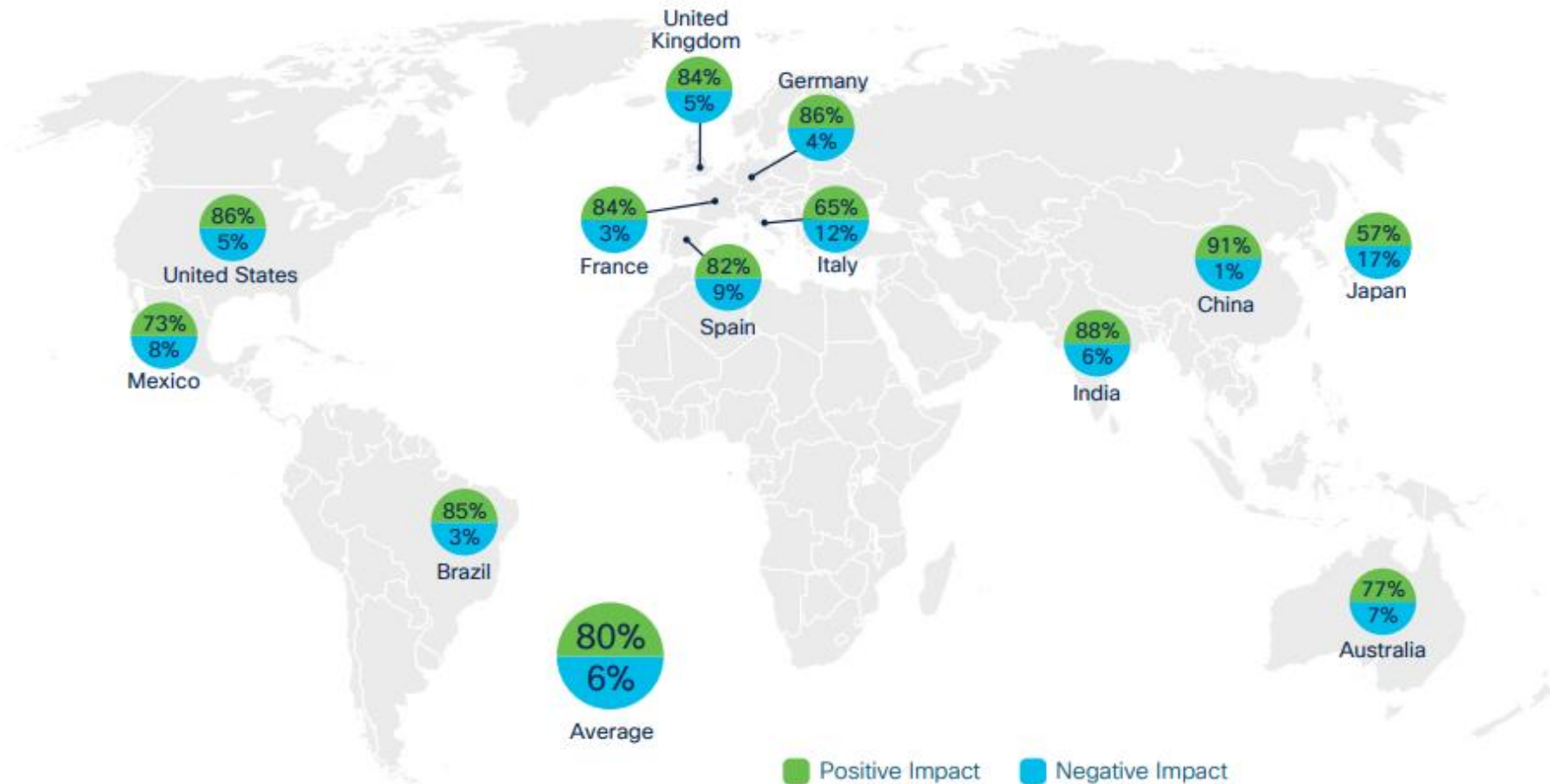
Source: Cisco 2024 Data Privacy Benchmark Study

Figure 19. GenAI controls



Source: Cisco 2024 Data Privacy Benchmark Study

Figure 5. Impact of privacy laws on organizations



Source: Cisco 2024 Data Privacy Benchmark Study

What can go wrong?

IBM

2024 Cost of Data Breach Report

- IBM (2024) Cost of Data Breach Report.
<https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec>

Global average total cost of a data breach

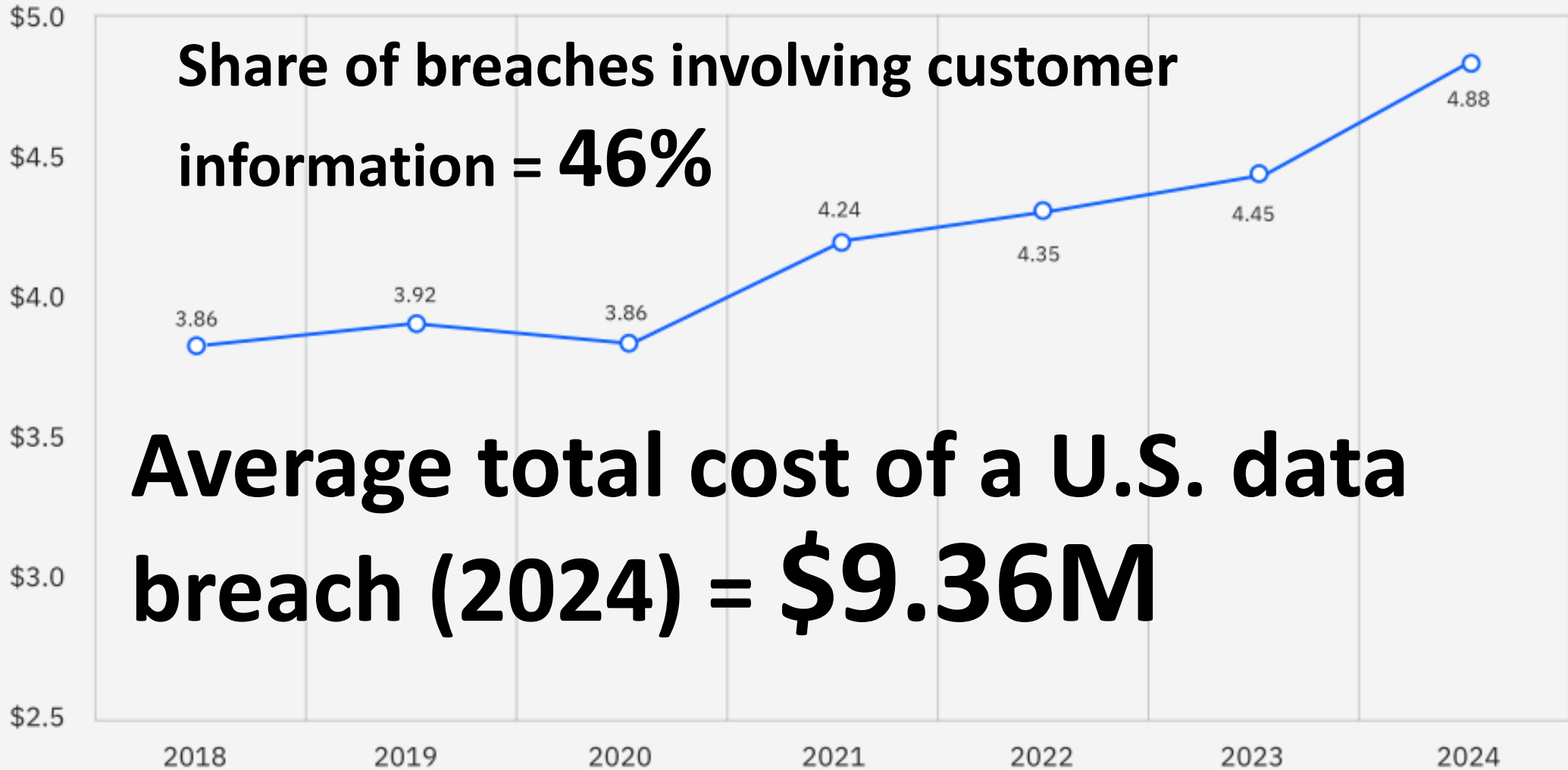


Figure 1. Measured in USD millions

Average cost of a data breach in 4 components

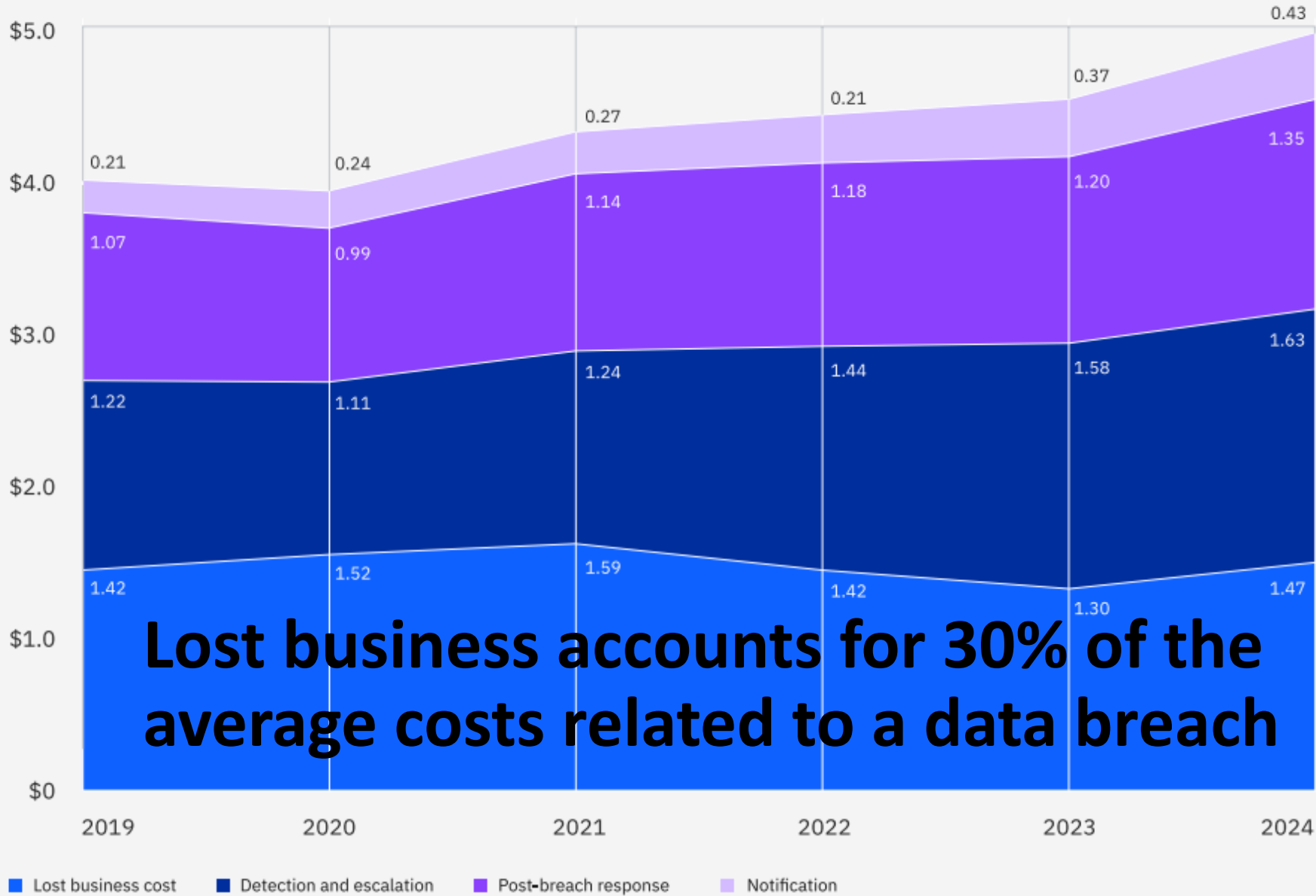


Figure 5. Measured in USD millions

The Top 50

BIGGEST DATA BREACHES



from 2004 - 2021

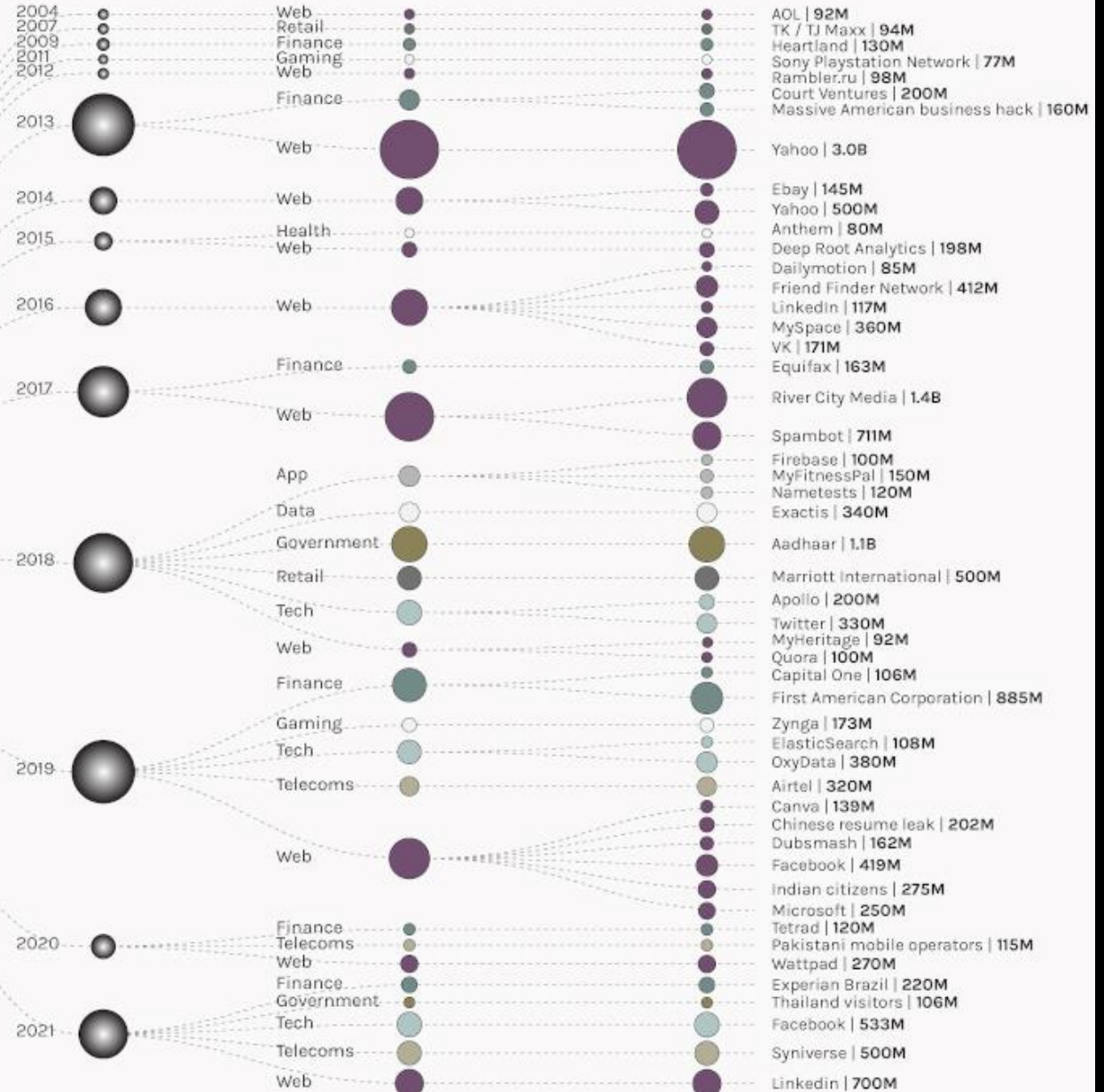
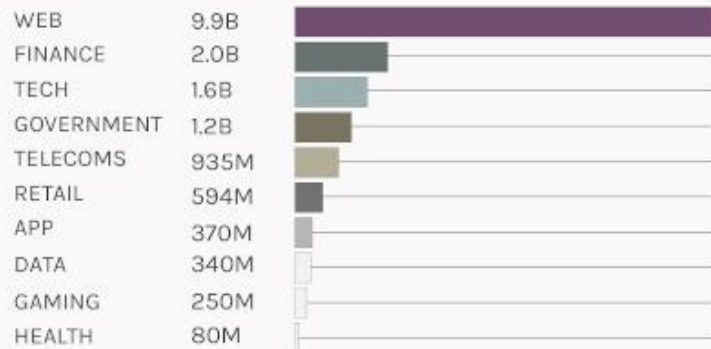
A data breach is an incident where protected information is copied, stolen, or exposed to an unauthorized person. The largest breach in recent times was the LinkedIn breach of 2021 in which 700 million records were lost. The visual on the right highlights the Top 50 known data breaches from 2004 to 2021. The Web sector was impacted the most. 9.9B records were lost. The Tech and Finance sectors were also severely impacted, and they lost 1.6B and 2.0B records, respectively.

SECTORS - These are industry sectors which the companies belong to. There are 10 in total.

17.2B

Total number of records lost

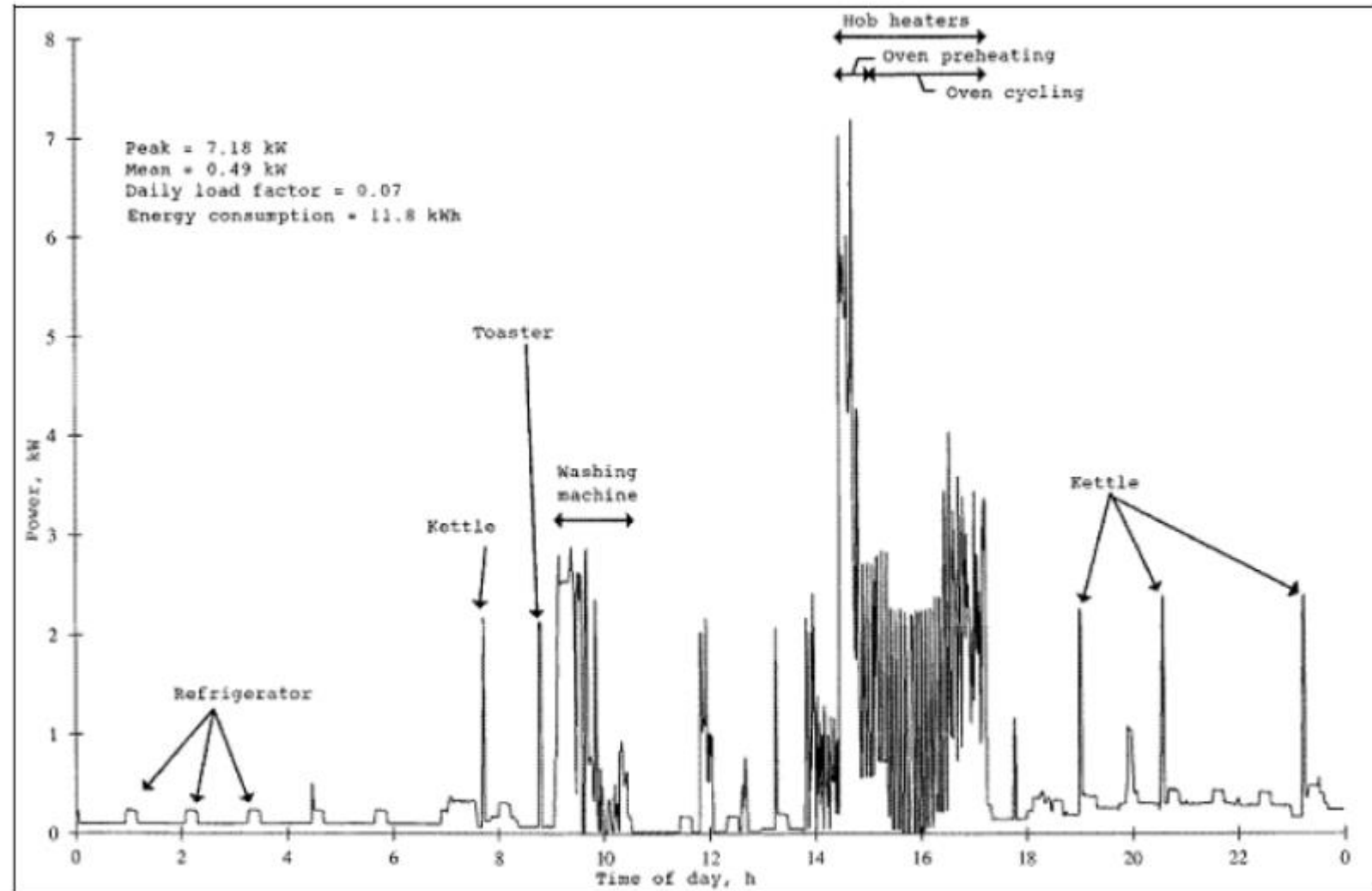
The number of records lost per sector is shown below:



Domestic Violence Concerns

- The ability for an abuser to keep tabs on a victim's electric usage data or be notified if service is about to be disconnected or that they are behind on payments can lead to harassment and potential life-threatening outcomes.

Figure 1: Identification of household activities from electricity usage data¹



¹ National Institute of Standards and Technology (2010) Guidelines for Smart Grid Cybersecurity: Vol. 2, Privacy and the Smart Grid 13 http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.

**Would Missouri be an outlier
if it adopted stronger
consumer protections?**

- As of July 2024, 20 US states have passed comprehensive data privacy laws, including laws that govern how businesses handle consumers' personal data:
 - California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, Texas, Florida, Montana, Oregon, Delaware, New Hampshire, New Jersey, Kentucky, Nebraska, and Rhode Island.
- Some utilities have been proactive. For example:
- ComEd's Anonymous Data Service provides customer-level interval usage data assembled for all customers (by customer delivery class) in a five-digit zip code. Specific retail customer identifiers, including but not limited to name, address, and electric account number, are omitted from the assembled data.

And some Commission's have been reactive:

2012 New York PSC Ruling against New York State Electric & Gas (NYSEG) and Rochester Gas and Electric (RG&E)

“Our investigation found that NYSEG and RG&E failed to meet industry standards and best practices to protect personally identifiable information of customers,” said Commission Chairman Garry Brown. “As a result, we are directing the companies to immediately take action to address the vulnerabilities on its computer billing and records systems currently used to take and maintain confidential customer information.” . . .

Based upon the investigation's findings, the companies should further refine policies, processes and procedures regarding confidentiality safeguards. The companies should minimize access to the most sensitive personally identifiable information by maintaining a strictly “need to know” standard for contractors and

employees alike. The companies should conduct, at least annually, an incident response exercise simulating a breach of such data. The companies should establish a protocol for notification of regulators in the event of any significant cyber incident involving a possible compromise of customer data; and the companies should promptly implement steps to ensure the security of all data stored on company mobile computers and removable data storage media. . .

In addition to the foregoing recommendations, the Commission raised concerns that the issue of costs that both the companies incur in responding to this security breach. The Commission will require the companies segregate and report all of the costs associated with rectifying the security breach, including the customer care costs identified above as well as any incremental investigation and remediation costs, as part of respective 2012 earnings sharing filings, and that the Commission closely scrutinize any proposal to incorporate these costs in the earnings sharing calculation. In this way, the companies will be put on notice that they will be required to justify fully the inclusion of any such expenses in their earnings sharing calculations.²⁰

- Platsky, J. (2012) Regulators criticize NYSEG for computer security breach. <http://www.thecre.com/fisma/?p=2145>

NARUC 2024 Mid-Year Resolution

I. Committee on Energy Resources and the Environment

Page 3

ERE-1 Resolution on Customer Energy Usage Data for Multi-Tenant Properties.....3

Sponsor: Davante Lewis, LA PSC [Version: 0712 139 PM vz from Commissioner Lewis]

The resolution encourages [1] state commissions [a] to identify opportunities and processes whereby owners of multi-tenant properties can access whole-building and tenant unit utility data in a standardized format, including aggregated building data that does not reveal customer-specific data to protect customer privacy; and [b] to request that utilities allow customers, including tenants of multi-tenant properties, to authorize the sharing of their usage information, with appropriate consent and privacy protections, with property owners, identified third parties, and implementers of federal programs and grants, to the extent provided for under State law and regulations and [2] utilities to develop procedures and methods to identify customer accounts associated with multi-tenant properties to facilitate property owners' access to available federal funding and other resources to reduce building-wide and tenant energy consumption.

Specifically states:

Whereas appropriate consumer protections are needed for any sharing of customer usage information, Customer usage information cannot be used for marketing or create data profiles to target customers for increasing profits. Customer data may only be disclosed to third parties with clear customer permission. Data protections and privacy safeguards are important for the preservation of public trust with DOE, utilities, and other programs;

Whereas States and utilities should develop simple mechanisms for customers to make educated decisions regarding the intentional authorization to disclose their energy data. In places where no such policy is in place, individual customers should be able to access their own data and disclose them to a third-party provider;

What is the OPC requesting?

Rules with an eye towards future-proofing emerging threats and safeguarding captive customers

- Customers want data privacy and more regulatory oversight
- Companies overwhelmingly see privacy laws and regulations as creating a positive impact to their bottom line
- Data breaches and associated costs are increasing year-over-year
- The potential privacy risks associated with AI cannot be overstated and are emerging at a rapid clip
- Customer consent, transparency in obtaining, storing, erasing data, and following a data minimization mindset will limit liability, build customer trust, and support the Commission's statutory directive to protect the public.

Take proposed rules and add the following:

1. Add a definition of “Aggregated Customer Information”
2. Add a definition of “Consent”
3. Add a definition and standard for “Utility Related Services”
4. Clarify subsection (2)(B)
5. Add a provision regarding the ownership of customer information
6. Enhance subsection (3) regarding notification of breaches
7. Add a provision requiring the filing of a Customer Data Privacy Policy

Questions?

Geoff Marke
Chief Economist
Missouri Office of the
Public Counsel

Geoff.marke@opc.mo.gov

12/10/2024