Ethical Considerations

CS 40 | March 4, 2024

GUEST LECTURE on Wednesday 3/6
by Corey Quinn, Chief Cloud Economist, Duckbill Group
MANDATORY ATTENDANCE

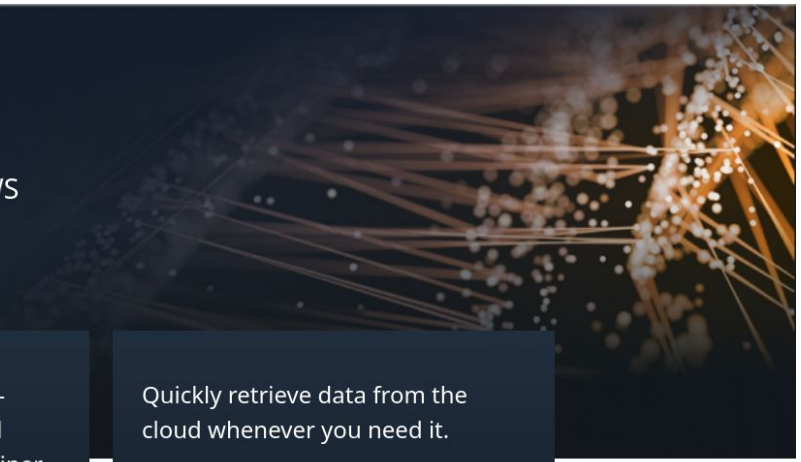
Assignment 4 Out (due Saturday 3/9)

« Storage

AWS Snowmobile

Migrate or transport exabyte-scale datasets into and out of AWS

Contact sales to order an AWS Snowmobile



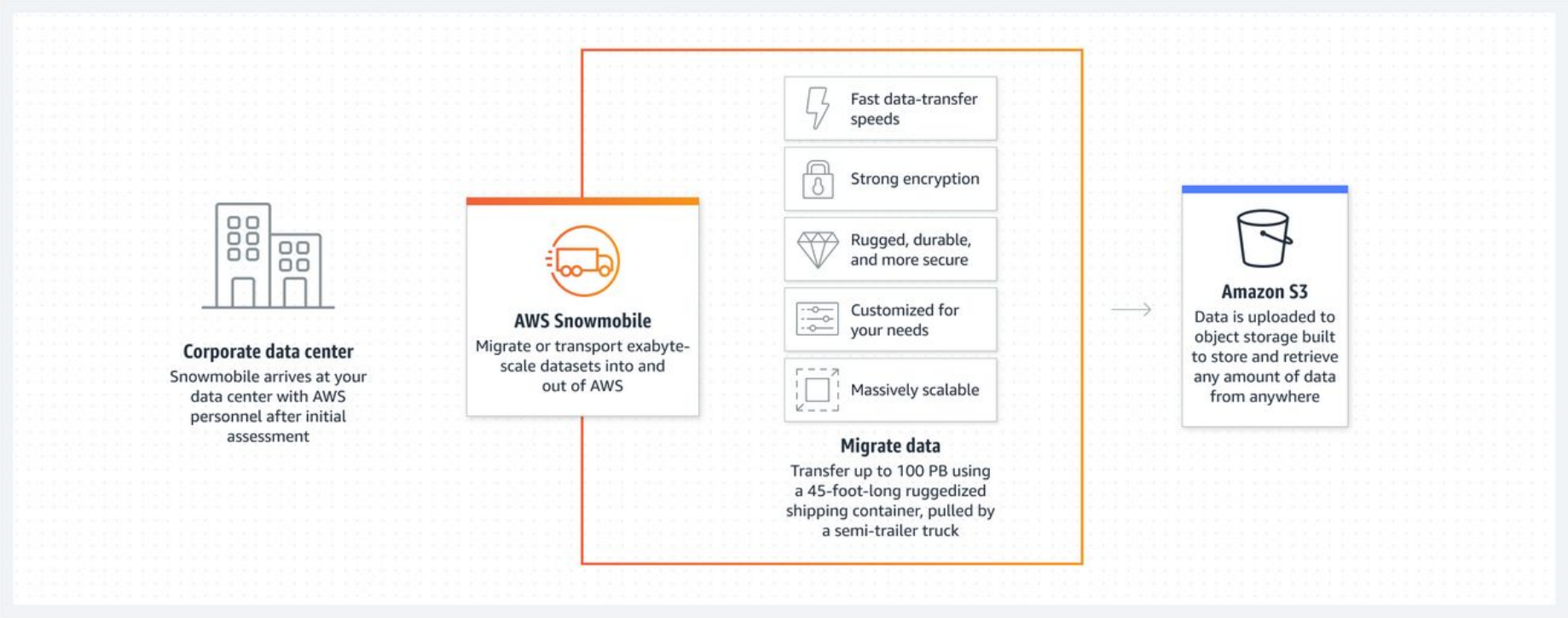
Quickly and securely transfer up to 100 petabytes of data in as little as a few weeks.

Protect your data in a tamper-resistant, water-resistant, and temperature-controlled container with limited physical access.

Quickly retrieve data from the cloud whenever you need it.

How it works

AWS Snowmobile moves extremely large amounts of data to AWS. Transfer up to 100 PB per Snowmobile, a 45-foot-long ruggedized shipping container pulled by a semi-trailer truck.



Click to enlarge

Agenda

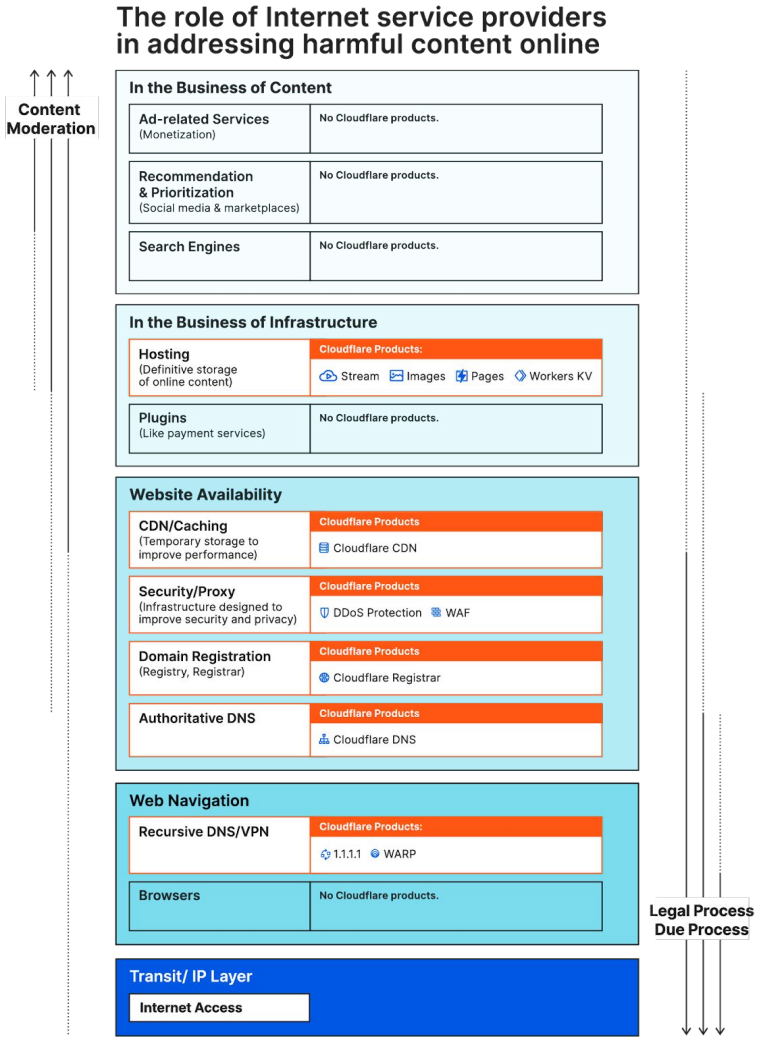
1. Centralization of Power
2. Law Enforcement Access to Data
3. Trusted Computing
4. Cybersecurity
5. Green Cloud Computing

Centralization of Power

By using a cloud provider, you give them some level of control over your business.

Kiwi Farms

- Background: Kiwi Farms is an *absolutely horrible* website dedicated solely to the doxing and abuse of trans people, resulting in at least one suicide
- In September 2022, Cloudflare withdrew DDoS protection from Kiwi Farms after reports of suicide due to continued harassment
- Argument: Cloudflare did not directly censor Kiwi Farms, merely declined further business



Parler

- Background: Parler is an *absolutely horrible* social media website dedicated solely to far right activism and extremism, including election denial

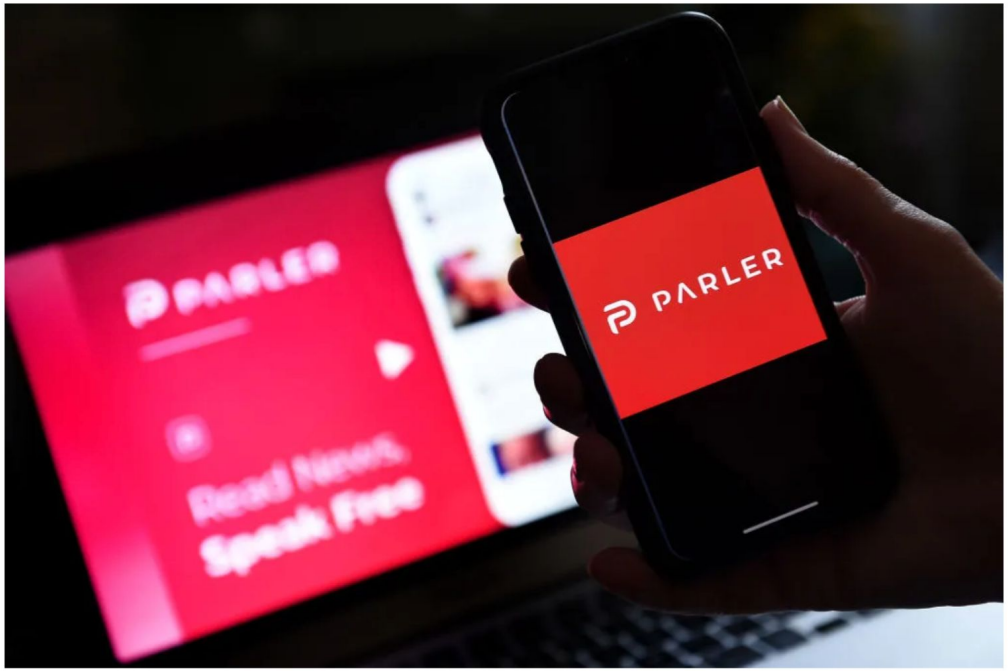
- In 2021, AWS bans Parler from its platforms
  - Parler goes down for a long time as it is forced to migrate cloud providers

- AWS unilaterally decided to prevent the continued operation of a website
  - Potentially concerning precedent, regardless of the ethical validity of the underlying action

TECH • INTERNET

Why Amazon's Move to Drop Parler Is a Big Deal for the Future of the Internet

5 MINUTE READ



This illustration picture shows social media application logo from Parler displayed on a smartphone with its website in the background in Arlington, Virginia on July 2, 2020. Olivier Douliery—AFP/Getty Images

BY ALEX FITZPATRICK JANUARY 21, 2021 3:06 PM EST

ISPs Should Not Police Online Speech—No Matter How Awful It Is.

BY ELECTRONIC FRONTIER FOUNDATION | AUGUST 29, 2023

Law Enforcement Access to Data

Relevant Legislation

- **Foreign Intelligence Surveillance Act (1978):** Formation of a special court (FISC) to approve government requests for surveillance warrants
  - Modified several times since
  - Modern court publishes statistics on its rulings
  - **PRISM**: government mass surveillance operation that was overseen by the FISC

- **Electronic Communications Privacy Act (1986)**: Series of rules outlining process for government collection of communications data

(Slightly Newer) Relevant Legislation

- **PATRIOT Act (2001):** Massively increased government surveillance powers
  - Response to 9/11
  - In some cases, no warrant required
  - **USA FREEDOM Act (2015)**: modifies some Patriot Act provisions, mostly a response to Snowden leaks and concerns about government overreach

- **CLOUD Act (2018):** Outlines methods for the US government to access data held overseas by US corporations
  - Mostly affects companies with overseas data

This article is more than **10 years old**

Edward Snowden: the whistleblower behind the NSA surveillance revelations

The 29-year-old source behind the biggest intelligence leak in the NSA's history explains his motives, his uncertain future and why he never intended on hiding in the shadows

Q&A with NSA whistleblower Edward Snowden: 'I do not expect to see home again'

NSA whistleblower Edward Snowden: 'I don't want to live in a society that does these sort of things'

ANALYSIS

Amazon Web Services: We'll go to court to fight gov't requests for data

By Nancy Gohring

Writer, ITworld | JUN 19, 2013 1:39 PM PST

Lavabit founder refused FBI order to hand over email encryption keys

Unsealed documents show Ladar Levison, now subject of government gag order, refused requests to 'defeat its own system'

Court ordered Levison to be fined $5,000 a day beginning 6 August until he handed over electronic copies of the keys. Photo: Demotix/Alex Milan Tracy/Corbis

Amazon’s Ring to Stop Letting Police Request Doorbell Video From Users

- Move dials back company’s longtime public-safety stance
- Law enforcement will now have to seek warrants for video

An Amazon.com Inc. Ring indoor camera. *Photographer: Chloe Collyer/Bloomberg*

By Matt Day

January 24, 2024 at 8:00 AM PST
Updated on January 24, 2024 at 10:59 AM PST

March 04, 2024

AWS to Launch an Infrastructure Region in the Kingdom of Saudi Arabia

AWS Region will enable customers to run workloads and securely store customer content in the Kingdom of Saudi Arabia while serving end users with even lower latency

New Region reflects AWS's long-term commitment to meeting high demand for cloud services in the Kingdom of Saudi Arabia and across the Middle East

AWS plans to invest more than $5.3 billion (approx. 19.88 billion SAR) in the Kingdom of Saudi Arabia

AWS will establish two new innovation centers and investment will include upskilling students, local developers, and the next generation of local talent at any stage in their career with access to cloud computing skills

End-to-End Encryption

- Encrypt all customer data so that not even you can view it
  - Encrypted data is sent from your DB to user's device, decrypted locally
  - Example implementation: Signal Protocol
- Consequences
  - Usability
  - Analytics
  - Legitimate law enforcement access
- Ways to configure for cloud services exist

Blog

February 21, 2024

iMessage with PQ3: The new state of the art in quantum-secure messaging at scale

Posted by Apple Security Engineering and Architecture (SEAR)

Trusted Computing

Cryogenically frozen RAM bypasses all disk encryption methods

Computer encryption technologies have all relied on one key assumption that RAM (Random Access Memory) is volatile and that all content is lost when power is lost. That key assumption is now being fundamentally challenged with a $7 can of compressed air and it's enough to give every security professional heart burn.

Written by **George Ou,** Contributor

Feb. 21, 2008 at 3:59 p.m. PT

Trusted Computing

- *Idea*: Have the underlying CPU carve out a secure area that even someone with physical access to the server cannot inspect
  - Have a method where the hardware can **attest** that you are running in a secure state
  - Works, as long as you can trust the hardware and the security

- Physical threat model: must be resilient even against an attacker physically connecting wires to the circuit board

- Examples:
  - Intel SGX/TDX
  - AMD SEV
  - ARM Trustzone

A Survey of Published Attacks on Intel SGX

Alexander Nilsson*†, Pegah Nikbakht Bideh*, Joakim Brorsson*‡§
{alexander.nilsson,pegah.nikbakht_bideh,joakim.brorsson}@eit.lth.se
*Lund University, Department of Electrical and Information Technology, Sweden
†Advenica AB, Sweden
‡Combitech AB, Sweden
§Hyker Security AB, Sweden

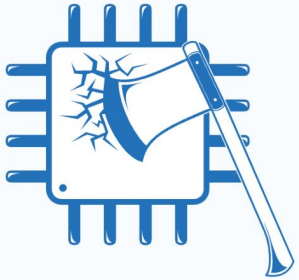
CacheOut

Leaking Data on Intel CPUs via Cache Evictions

We present CacheOut, a new speculative execution attack that is capable of leaking data from Intel CPUs across many security boundaries. We show that despite Intel's attempts to address previous generations of speculative execution attacks, CPUs are still vulnerable, allowing attackers to exploit these vulnerabilities to leak sensitive data.

Moreover, unlike previous MDS issues, we show in our work how an attacker can exploit the CPU's caching mechanisms to select what data to leak, as opposed to waiting for the data to be available. Finally, we empirically demonstrate that CacheOut can violate nearly every hardware-based security domain, leaking data from the OS kernel, co-resident virtual machines, and even SGX enclaves.

Read the Paper | Cite



SGAxe

How SGX Fails in Practice

SGAxe is an evolution of CacheOut, specifically targeting SGX enclaves. We show that despite extensive efforts done by Intel in order to mitigate SGX side channels, an attacker can still breach the confidentiality of SGX enclaves even when all side channel countermeasures are enabled.

We then proceed to show an extraction of SGX private attestation keys from within SGX's quoting enclave, as compiled and signed by Intel. With these keys in hand, we are able to sign fake attestation quotes, just as if these have initiated from trusted and genuine SGX enclaves. This erodes trust in the SGX ecosystem, as using such quotes an attacker can masquerade itself as a genuine SGX enclave to a remote party, while offering little protection in reality.

Read the Paper | Cite

How Stuff Gets eXposed

Intel's Software Guard Extension (SGX) promises an isolated execution environment, protected from all software running on the machine. In the past few years, however, SGX has come under heavy fire, threatened by numerous side channel attacks. With Intel repeatedly patching SGX to regain security, we set out to explore the effectiveness of SGX's update mechanisms to prevent attacks on real-world deployments.

More specifically, we survey and categorize various SGX attacks, their applicability to different SGX architectures, as well as the information they leak. We then explored the effectiveness of SGX's update mechanisms in preventing attacks on two real-word deployments, the SECRET network and PowerDVD. In both cases, we show that these vendors are unable to meet the security goals originally envisioned for their products, presumably due to SGX's long update timelines and the complexities of a manual update process. This forces vendors to make a difficult security vs. usability trade off, resulting in security compromises.

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

RAIDING FORT KNOX —

SGX, Intel's supposedly impregnable data fortress, has been breached yet again

ÆPIC Leak spills users' most sensitive secrets in seconds from SGX enclaves.

DAN GOODIN - 8/9/2022, 10:01 AM

CacheWarp Attack: New Vulnerability in AMD SEV Exposes Encrypted VMs

Nov 14, 2023 Newsroom

A group of academics has disclosed a new "software fault attack" on AMD's Secure Encrypted Virtualization (SEV) technology that could be potentially exploited by threat actors to infiltrate encrypted virtual machines (VMs) and even perform privilege escalation.

Secure Enclaves

- *Idea*: Have a *coprocessor* attest that you communicating with a trusted resource, delegate all cryptographic operations to it

- Lower scope than SGX/SEV/etc
  - Not trying to secure whole system, only a coprocessor
  - Lower attack surface
  - Fewer guarantees for you

- Examples: Apple Secure Enclave, Intel Managment Engine/AMD Platform Secure Processor, AWS Nitro Enclave, Google Titan/Titan M, Microsoft Pluton

Cybersecurity

Side-Channel Attacks

- **Definition**: Exploiting unintended information leakage to infer sensitive data being processed by the CPU

- Fundamental issue: the cloud is shared with other (untrusted) entities
  - Cloud provider must provide isolation between customers
  - Hard (impossible?) to guarantee this separation

Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds

Thomas Ristenpart[*] Eran Tromer[†] Hovav Shacham[*] Stefan Savage[*]

[*]Dept. of Computer Science and Engineering
University of California, San Diego, USA
{tristenp,hovav,savage}@cs.ucsd.edu

[†]Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology, Cambridge, USA
tromer@csail.mit.edu

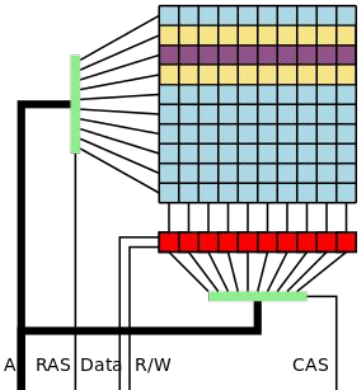
Meltdown and Spectre (2018)

- Series of side channel vulnerabilities that allows for the reading of privileged memory by abusing speculative execution capabilities of modern CPUs

- Mostly mitigated in hardware, but will haunt computing industry for a long time
  - *Very difficult* to completely mitigate: attacks the fundamental design of modern CPUs

Rowhammer

- Rowhammer: hardware vulnerability that exploits the repeated access of memory cells to induce electrical interference, causing unintended bit flips in adjacent memory rows
    - An attacker with the ability to write to adjacent rows may be able to change the values of your memory



- Abuses the physical properties of memory

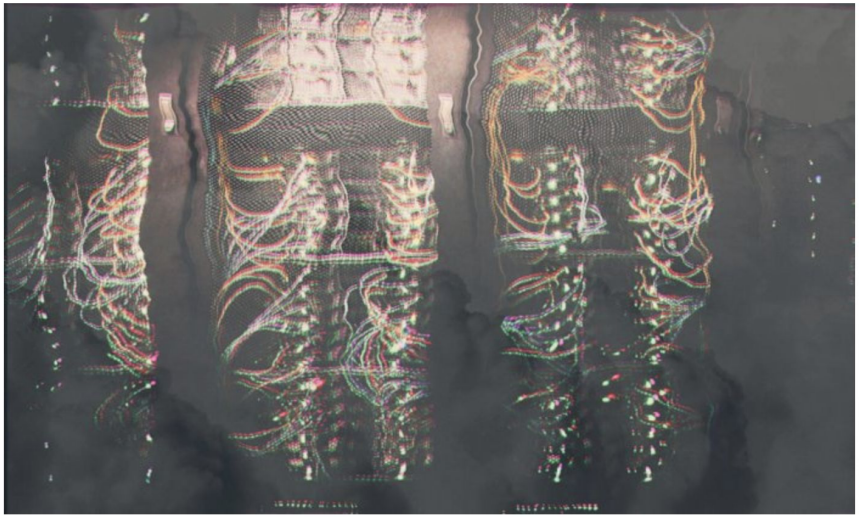
The Bottom Line

- No way for you to directly mitigate any of these (or many others)
- Using a cloud system shared with other people carries inherent risks
- Should you trust your user's data to a cloud you may not be able to trust?

Green Cloud Computing

The Staggering Ecological Impacts of Computation and the Cloud

Anthropologist Steven Gonzalez Monserrate draws on five years of research and ethnographic fieldwork in server farms to illustrate some of the diverse environmental impacts of data storage.



The Cloud is not only material, but is also an ecological force. Source image: Taylor Vick, via Unsplash

By: Steven Gonzalez Monserrate

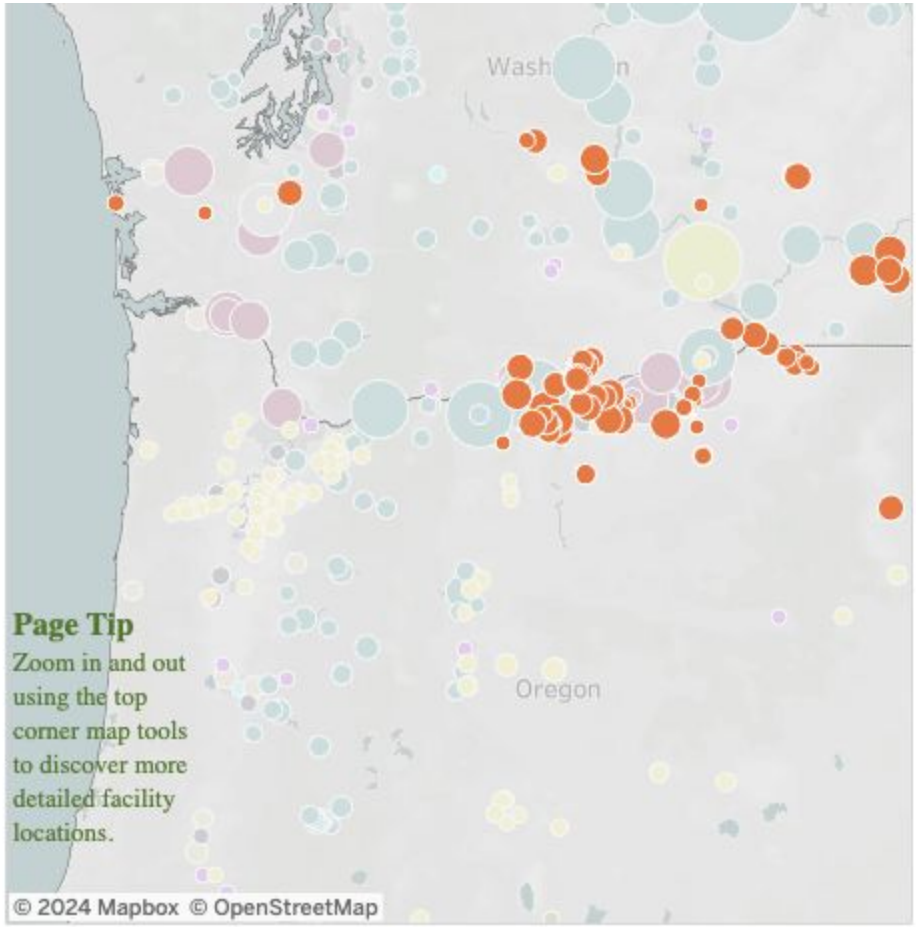
CO2 Footprint

- Very high
  - More than entire aviation industry
  - Potentially mid single digits of *total world CO2 emissions*

Cloud Provider Argument

- Cloud is more efficient than individual data centers
  - "between 22% and 93% more efficient than traditional enterprise data centers" – Microsoft
  - "running business applications on AWS, rather than on-premises enterprise datacenters in Europe, could reduce associated energy usage by nearly 80% and carbon emissions by up to 96%" – AWS

- Economics of scale, ability to invest and demand sources of green energy



Resource

- Wind
- Solar
- Coal
- Nuclear
- Hydro
- Natural Gas
- Geothermal
- Biogas
- Other Fuels
- Biomass
- Petroleum

Generating Site Owner

(All)

Next Lecture: Cloud Billing Concerns (3/6) GUEST LECTURE by Corey Quinn, Chief Cloud Economist, Duckbill Group MANDATORY ATTENDANCE