# Software Security and Privacy: A Geopolitical Perspective

PRESENTER

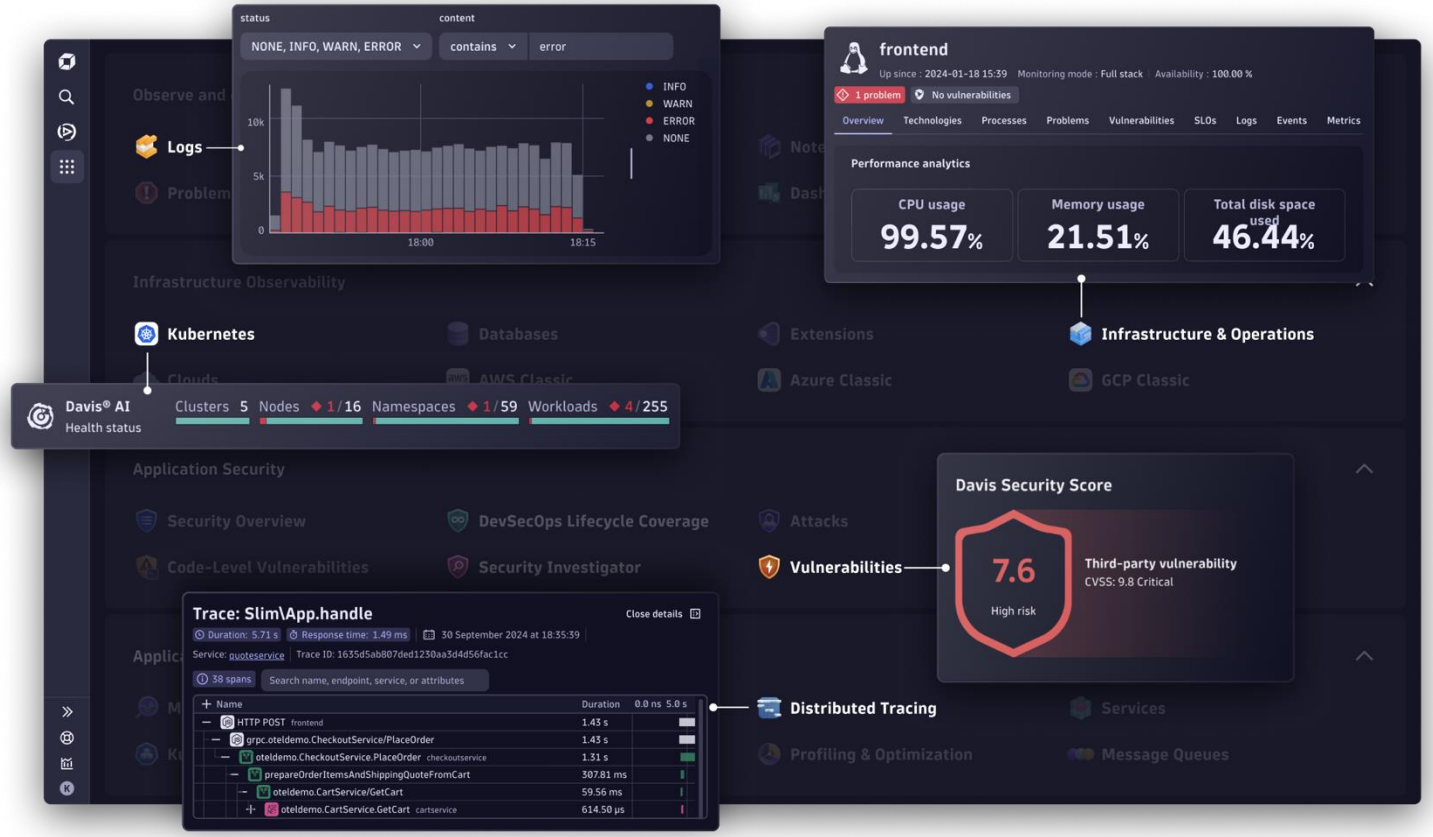
**Cat Easdon**
Senior Privacy Engineer &
Team Captain

# whoami

- Lead Dynatrace's Privacy Engineering team in close collaboration with our Product Security teams
- ⛰️-obsessed Brit based in Innsbruck
- Engineering background, but my work has drawn me towards politics and policy
  - Tech policy (Virtual Routes, Internet Society)
  - Side-channel attacks and backdoors (TU Graz)
  - Privacy and civil liberties (Palantir)

# My day-to-day perspective on security and privacy

**Dynatrace:** observability platform with ~$1.5 billion ARR and ~4000 customers including BT, EDF Energy, National Grid, Deutsche Telekom, TSB, Allianz, Air Canada, Walmart, State of Minnesota

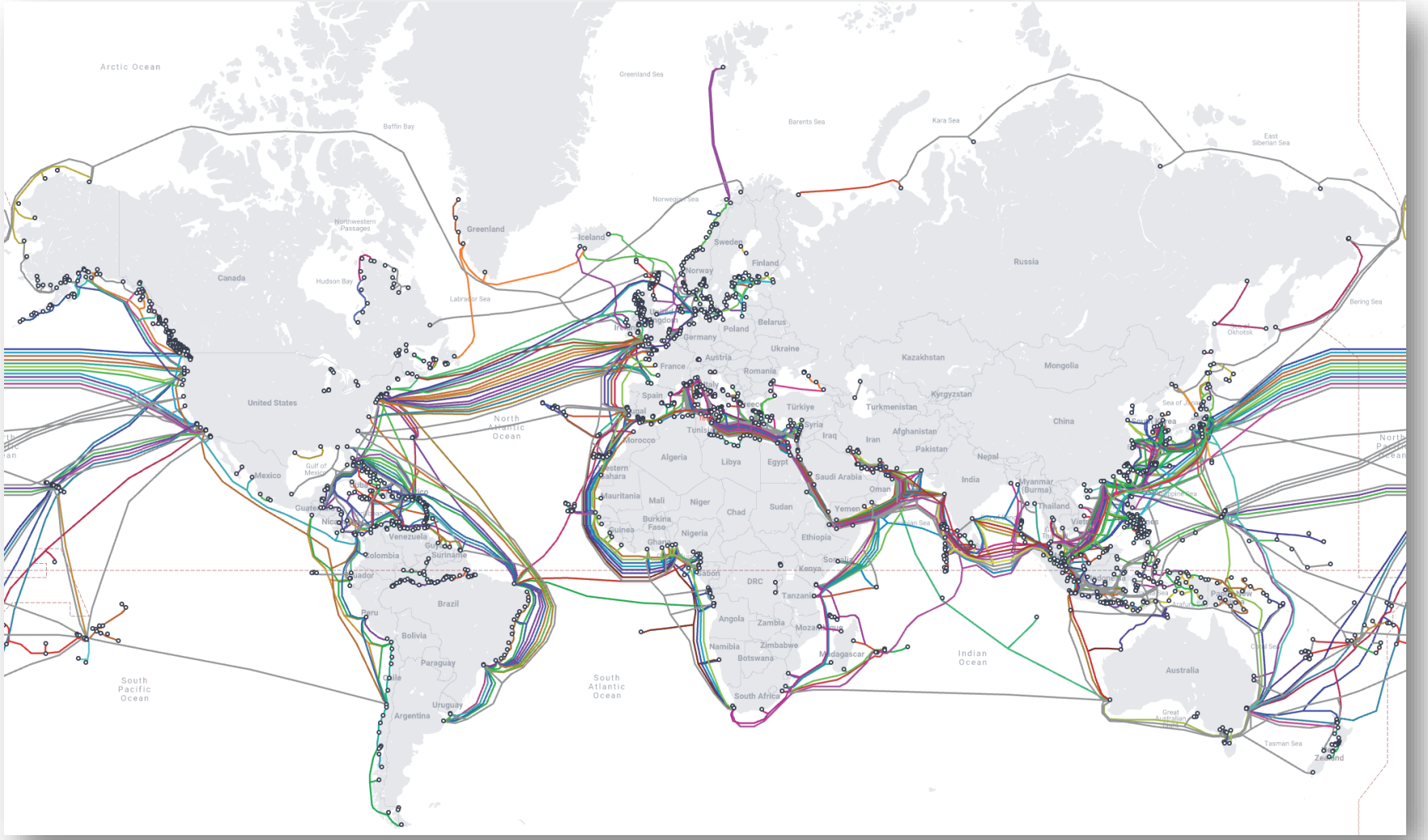


# Disclaimer

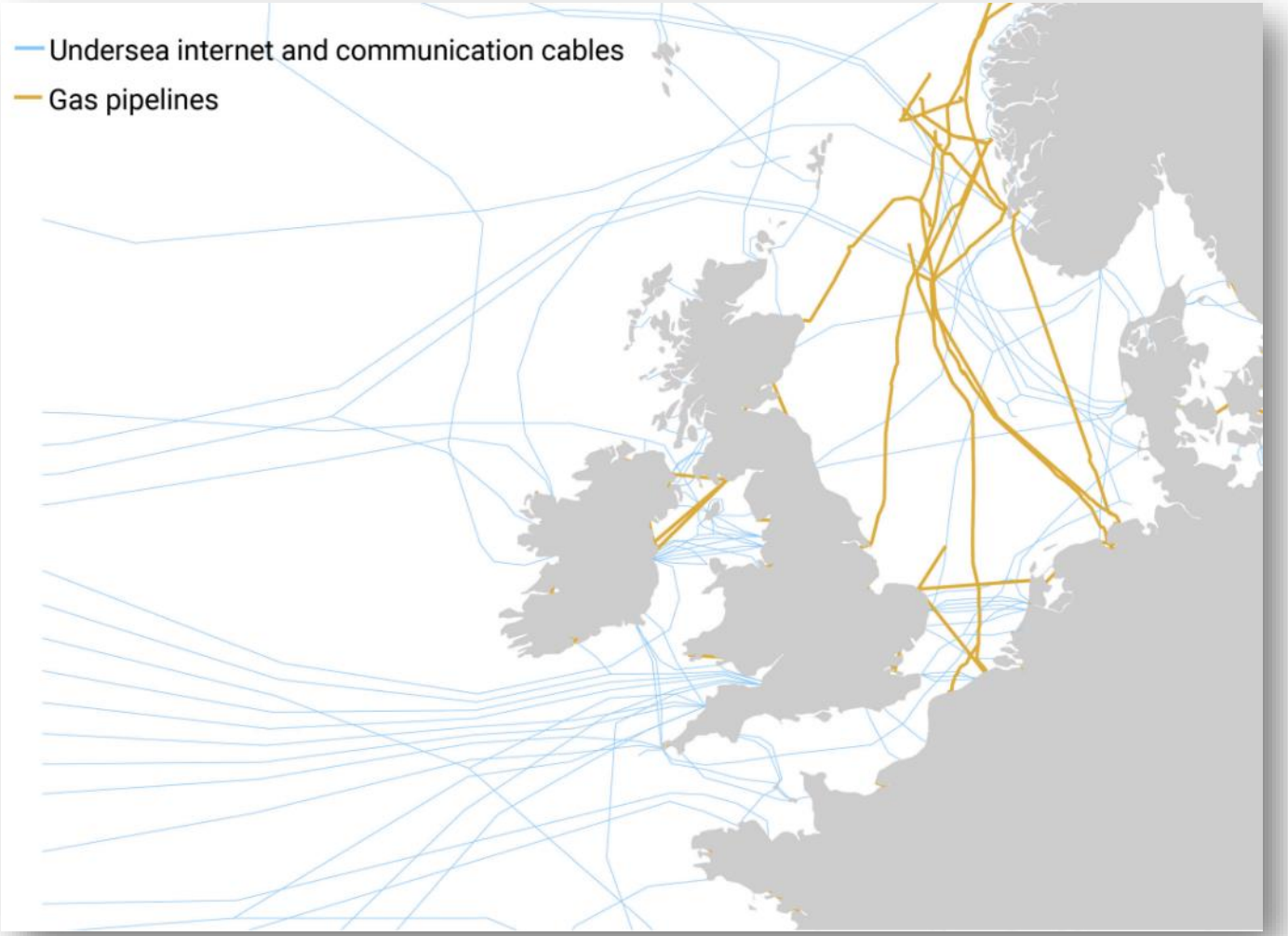
*"In our age there is no such thing as 'keeping out of politics.' All issues are political issues, and politics itself is a mass of lies..." ~ George Orwell, 1941*

- I will try to do the impossible today and make geopolitics relatively unpolitical!
- Opinions and recommendations are my own and not those of Dynatrace or the Security Forum

# Geopolitics? In software?!



# Geopolitics? In software?!



# Security and privacy: two pieces of the geopolitical puzzle

2. There are some undocumented internal-use MSRs used for low-level hardware testing purposes. Attempts to read or write these undocumented MSRs cause unpredictable and disastrous results; so don't use MSRs that are not documented in this datasheet!

**No Fix** | **Processor May Hang Under Complex Scenarios**

EDI=9C5A203A

activates 4 debug MSRs on AMD K7

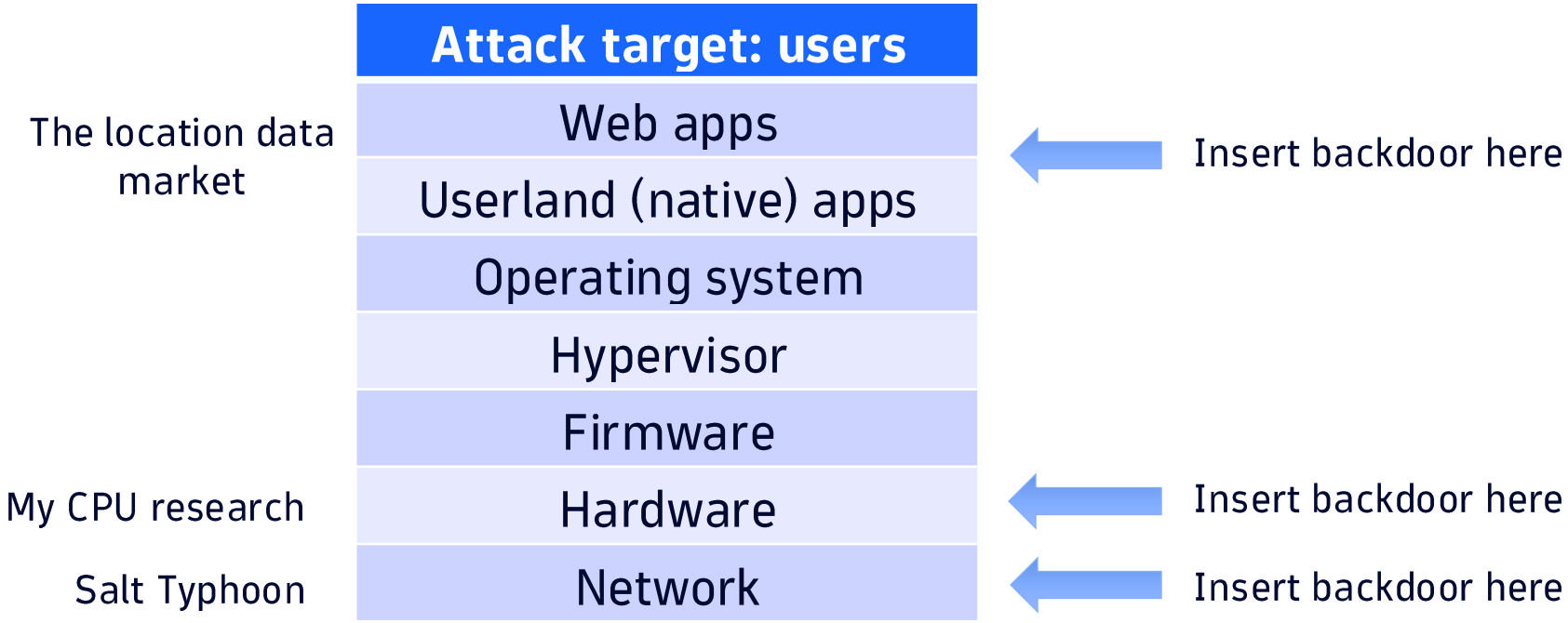
This page was intentionally left blank.

# Security and privacy: two pieces of the geopolitical puzzle

```
U32f0: 002165071408                tmp1:= CONCAT_DSZ32(0x04040404)
U32f1: 004700031c75                tmp1:= NOTAND_DSZ64(tmp5, tmp1)
U32f2: 006501031231                tmp1:= SHR_DSZ64(tmp1, 0x00000001)
            01c4c980               SEQW GOTO U44c9
-------------------------------------------------------------------------------

U32f4: 0251f25c0278                UJMPCC_DIRECT_NOTTAKEN_CONDNS(tmp8, U37f2)
U32f5: 006275171200                tmp1:= MOVEFROMCREG_DSZ64( , PMH_CR_EMRR_MASK)
U32f6: 186a11dc02b1                BTUJB_DIRECT_NOTTAKEN(tmp1, 0x0000000b, generate_#GP) !m0,m1
            01e15080               SEQW GOTO U6150
-------------------------------------------------------------------------------

U32f8: 000c85e80280                SAVEUIP( , 0x01, U5a85) !m0
U32f9: 000406031d48                tmp1:= AND_DSZ32(0x00000006, tmp5)
U32fa: 1928119c0231                CMPUJZ_DIRECT_NOTTAKEN(tmp1, 0x00000002, generate_#GP) !m0,m1
            0187bd80               SEQW GOTO U07bd
-------------------------------------------------------------------------------

U32fc: 00251a032235                tmp2:= SHR_DSZ32(tmp5, 0x0000001a)
U32fd: 0062c31b1200                tmp1:= MOVEFROMCREG_DSZ64( , 0x6c3)
U32fe: 000720031c48                tmp1:= NOTAND_DSZ32(0x00000020, tmp1)
            01c4d580               SEQW GOTO U44d5
-------------------------------------------------------------------------------
```

# Security and privacy: two pieces of the geopolitical puzzle

# Security and privacy: two pieces of the geopolitical puzzle



# A Security Wartime Mindset

# “I’ll be honest: the security situation does not look good.”


*“It’s undoubtedly the worst in my lifetime. And I suspect in yours too.”*

## “I’ll be honest: the security situation does not look good.”

Elon Musk says he withheld Starlink over Crimea to avoid escalation BBC

## “I’ll be honest: the security situation does not look good.”

Elon Musk says he withheld Starlink over Crimea to avoid escalation BBC

TIME

The Collapse of Global Arms Control

# “I’ll be honest: the security situation does not look good.”

Elon Musk says he withheld Starlink over Crimea to avoid escalation BBC

TIME
The Collapse of Global Arms Control

Dutch parliament calls for end to dependence on US software companies Reuters

# “I’ll be honest: the security situation does not look good.”

Elon Musk says he withheld Starlink over Crimea to avoid escalation BBC

TIME
The Collapse of Global Arms Control

Dutch parliament calls for end to dependence on US software companies Reuters

The era of globalisation as we know it 'has come to an end', UK minister says The Guardian

# “I’ll be honest: the security situation does not look good.”

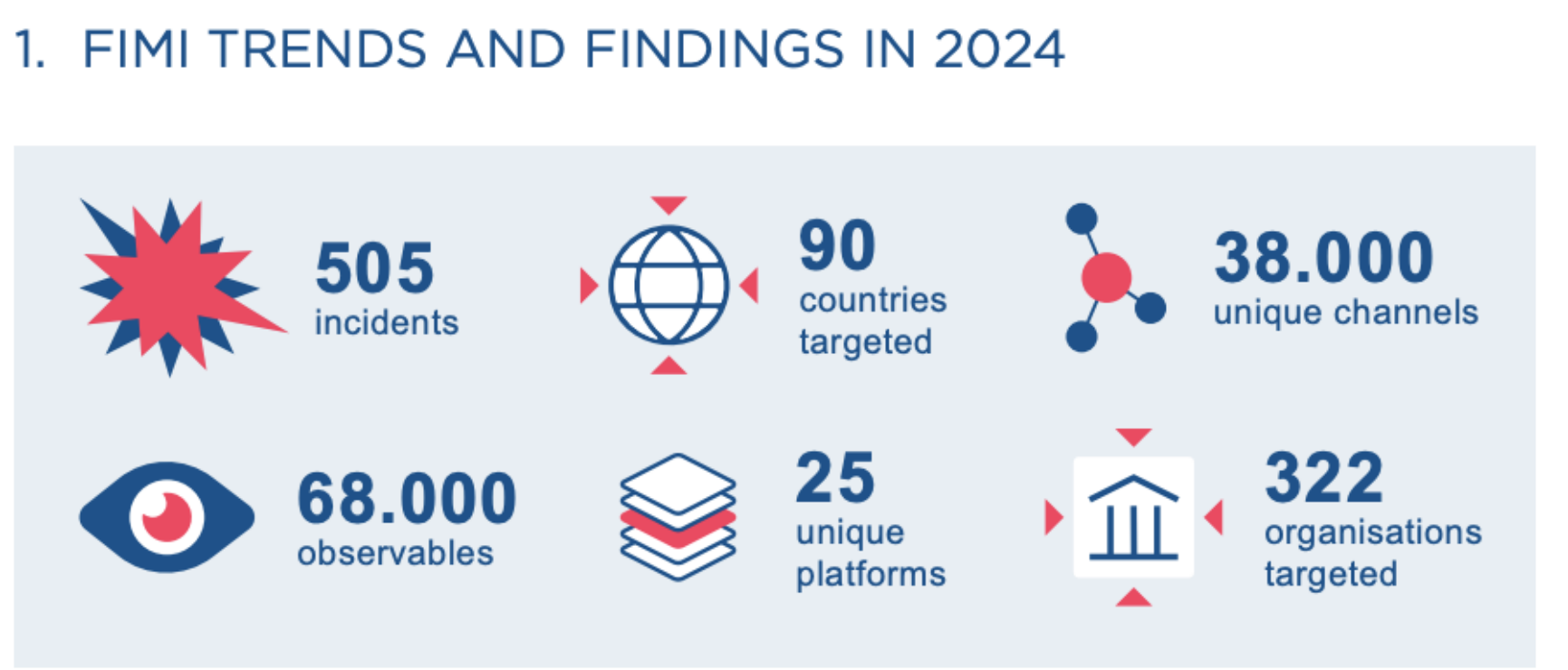



**Figure 1:** Key figures of findings across 2024 incidents

*“Our information space has become a geopolitical battleground.”*

# “I’ll be honest: the security situation does not look good.”


*“It is time to shift to a wartime mindset.”*

# What does a wartime mindset mean for us?

# What does a wartime mindset mean for us?

## Cybercriminals

Ransom for cash (paid by nation states)

## Private sector offensive actors (PSOA)

Spy for cash (paid by nation states)

## Nation states and aligned groups

- Destabilize and coerce
- Gather intel for strategic planning

# Destabilization case study: Synnovis ransomware attack

*"One of the most significant and harmful cyber attacks ever seen in the UK"*

- Targeted a pathology provider to disrupt hospitals in South East London for several weeks: 814 operations and 3000 appointments postponed, 400GB patient data leaked
- Urgent appeal for type-O blood donations; student volunteers delivered blood samples and test results by hand
- Restoring all digital clinical services took 5 months (without back-office systems)

Sources: BBC, The Record, Synnovis, FT

# What does a wartime mindset mean for us?

## Cybercriminals

Ransom for cash (paid by nation states)

## Private sector offensive actors (PSOA)

Spy for cash (paid by nation states)

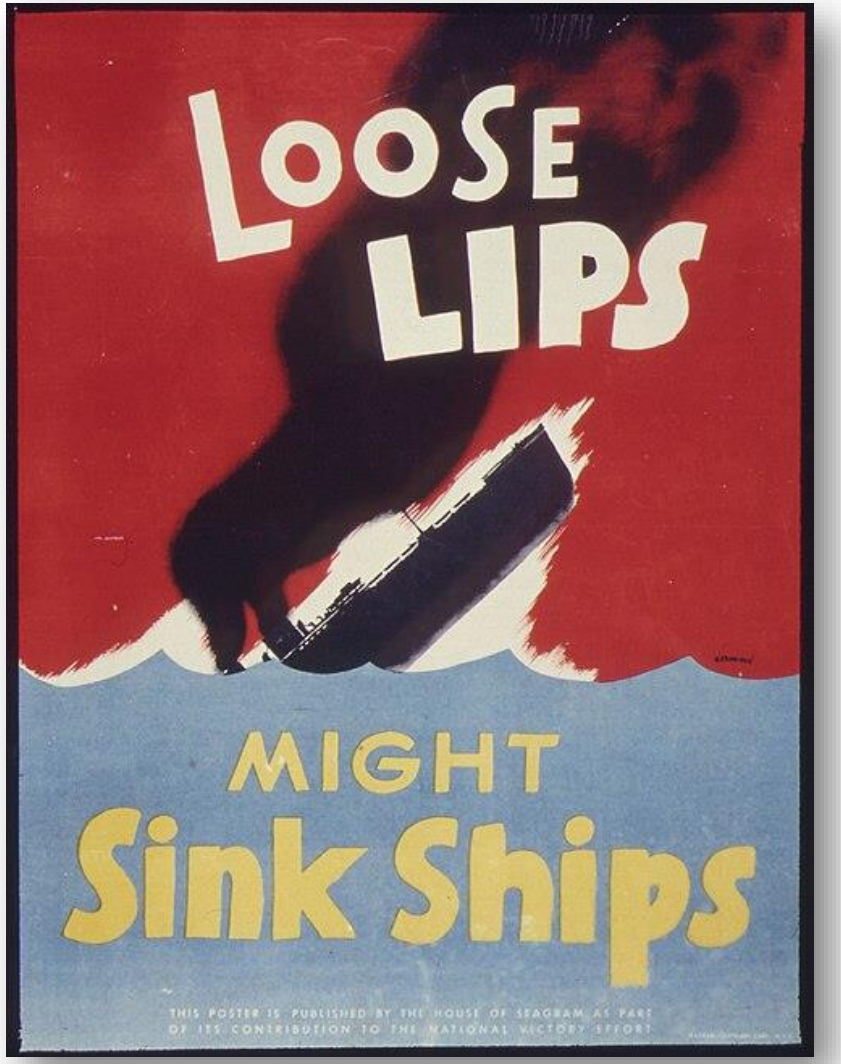
## Nation states and aligned groups

- Destabilize and coerce
- Gather intel for strategic planning

Our focus today

# Case Study 1: How might an app accidentally threaten national security?

# By leaking data!



# Strava heatmap (2018): military personnel go jogging too

# Volkswagen location data breach (2024): spies drive cars too…

# ...As do military counter-intelligence personnel

# Volkswagen location data breach (2024)

*For customers, there is "no need to do anything, since no sensitive data like passwords or payment information was affected."*

Volkswagen's statement to Der Spiegel

# “No sensitive data”

## Cybercriminals

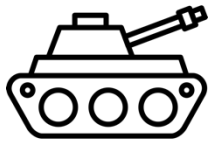
Ransom for cash (paid by nation states)

## Private sector offensive actors (PSOA)

Spy for cash (paid by nation states)

## Nation states and aligned groups

- Destabilize and coerce
- Gather intel for strategic planning



# Case Study 2: Gravy Analytics (Unacast) and the Location Data Market

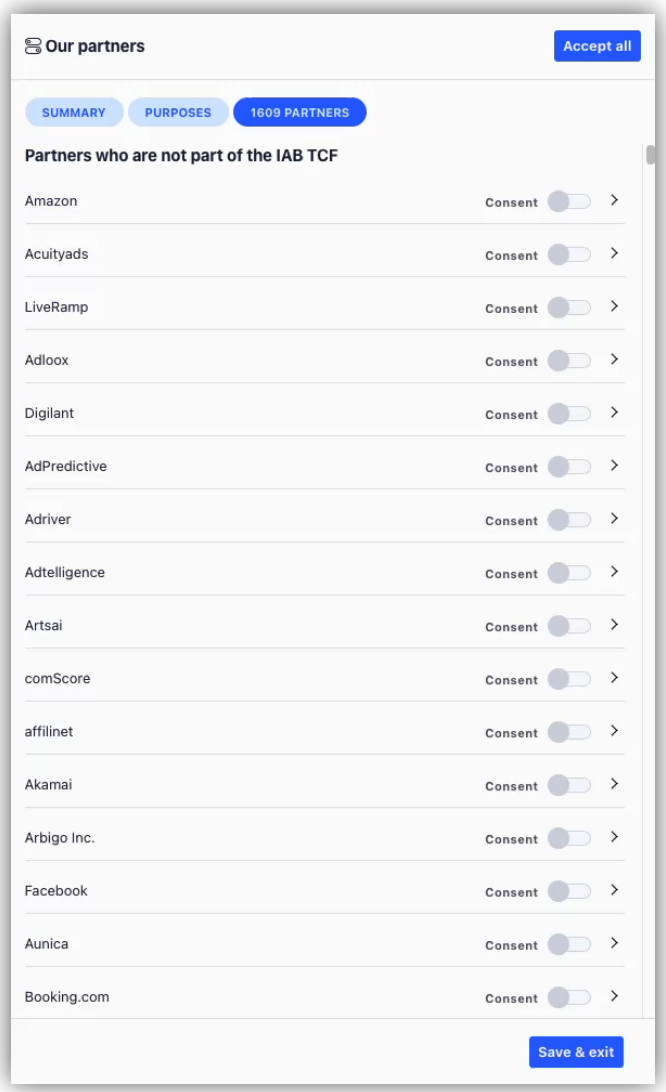
# Security and privacy: two pieces of the geopolitical puzzle

**The location data market**

| Attack target: users |
| --- |
| Web apps |
| Userland (native) apps |
| Operating system |
| Hypervisor |
| Firmware |
| Hardware |
| Network |

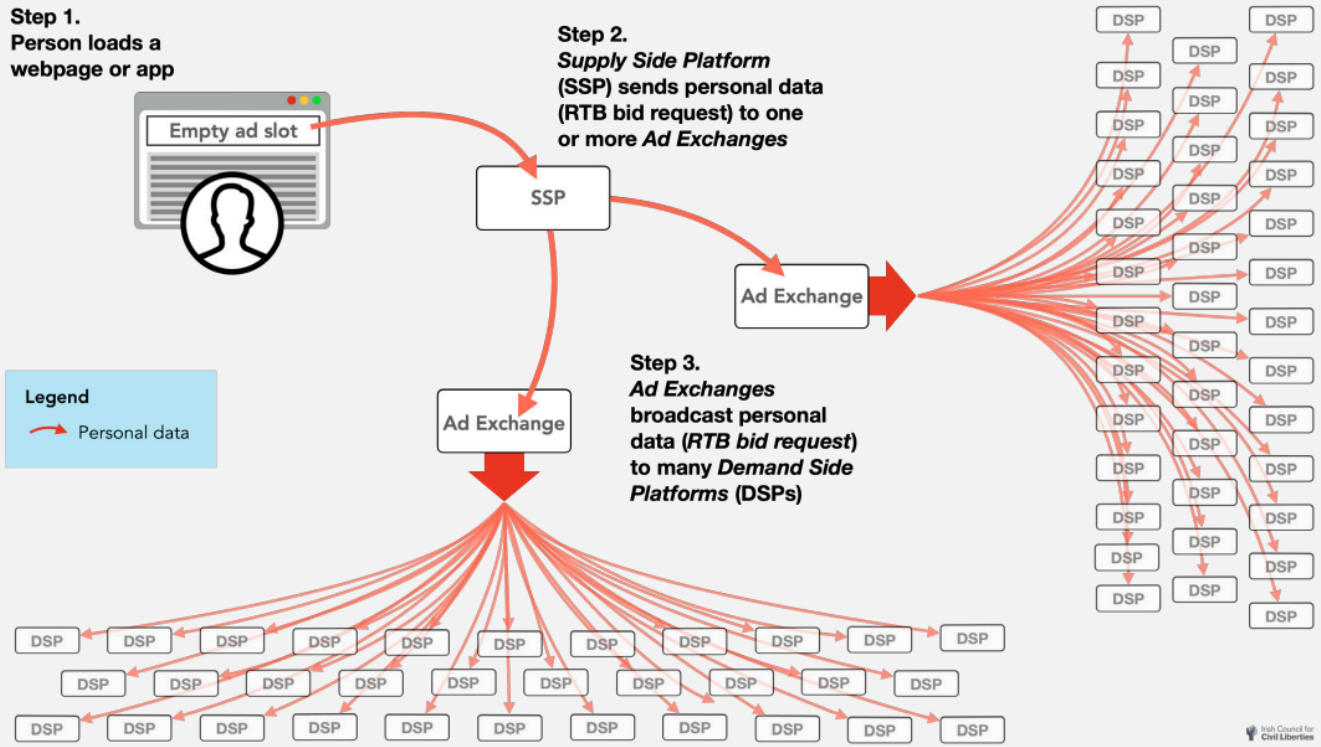
Insert backdoor here

# Ads, glorious ads!



# Displaying ads broadcasts your users' data to the world

The sale of a single ad slot often involves an auction of auctions, with several ad exchanges running competing auctions that are coordinated by a Supply Side Platform (SSP). This increases the number of DSPs that receive the broadcasted data.



# What is this data used for?

- Where's the best location to open a new shop?
- Where do our customers travel from?
- What's the value of this real estate?
- Is our ad campaign reaching the right people?
- In which city is a new hospital most urgently needed?
- How could we reduce traffic congestion in this neighborhood?
- How do people behave when forest fires start? How could we evacuate them faster?

# ...And other uses

Last November, Michael Morell, a former deputy director of the Central Intelligence Agency, hinted at a big change in how the agency now operates. "The information that is available commercially would kind of knock your socks off," Morell said in an appearance on the NatSecTech podcast. "If we collected it using traditional intelligence methods, it would be top secret-sensitive. And you wouldn't put it in a database, you'd keep it in a safe." WSJ

# Gravy Analytics location data breach (2025)

## What data was involved in the security incident?

The security incident involved commercially available data. A limited subset of this data, covering primarily a few days around New Year's 2025, was briefly posted on a dark web forum. The data we license mostly consists of mobile advertising IDs (MAIDs), longitude/latitude, and timestamps. **We do not receive information that can directly identify specific people, and we have no reasonable ability to identify any person.**

Our analysis of the data posted shows that most of the data consists of unlinked data elements that cannot be associated with any device. Even when a MAID is linked to location data, associating a specific person with any of this data would demand significantly more processing and supplementary datasets. The potential for tracking or profiling any person with this data is further limited by the restricted time span it covers. Harm is unlikely as a direct result of this incident.

# Gravy Analytics location data breach (2025)

30.4 **million** locations

## What data was involved in the security incident?

The security incident involved commercially available data. A limited subset of this data, covering primarily a few days around New Year's 2025, was briefly posted on a dark web forum. The data we license mostly consists of mobile advertising IDs (MAIDs), longitude/latitude, and timestamps. **We do not receive information that can directly identify specific people, and we have no reasonable ability to identify any person.**

Our analysis of the data posted shows that most of the data consists of unlinked data elements that cannot be associated with any device. Even when a MAID is linked to location data, associating a specific person with any of this data would demand significantly more processing and supplementary datasets. The potential for tracking or profiling any person with this data is further limited by the restricted time span it covers. Harm is unlikely as a direct result of this incident.

# Gravy Analytics location data breach (2025)

30.4 **million** locations

## What data was involved in the security incident?

The security incident involved commercially available data. A limited subset of this data, covering primarily a few days around New Year's 2025, was briefly posted on a dark web forum. The data we license mostly consists of mobile advertising IDs (MAIDs), longitude/latitude, and timestamps. **We do not receive information that can directly identify specific people, and we have no reasonable ability to identify any person.**

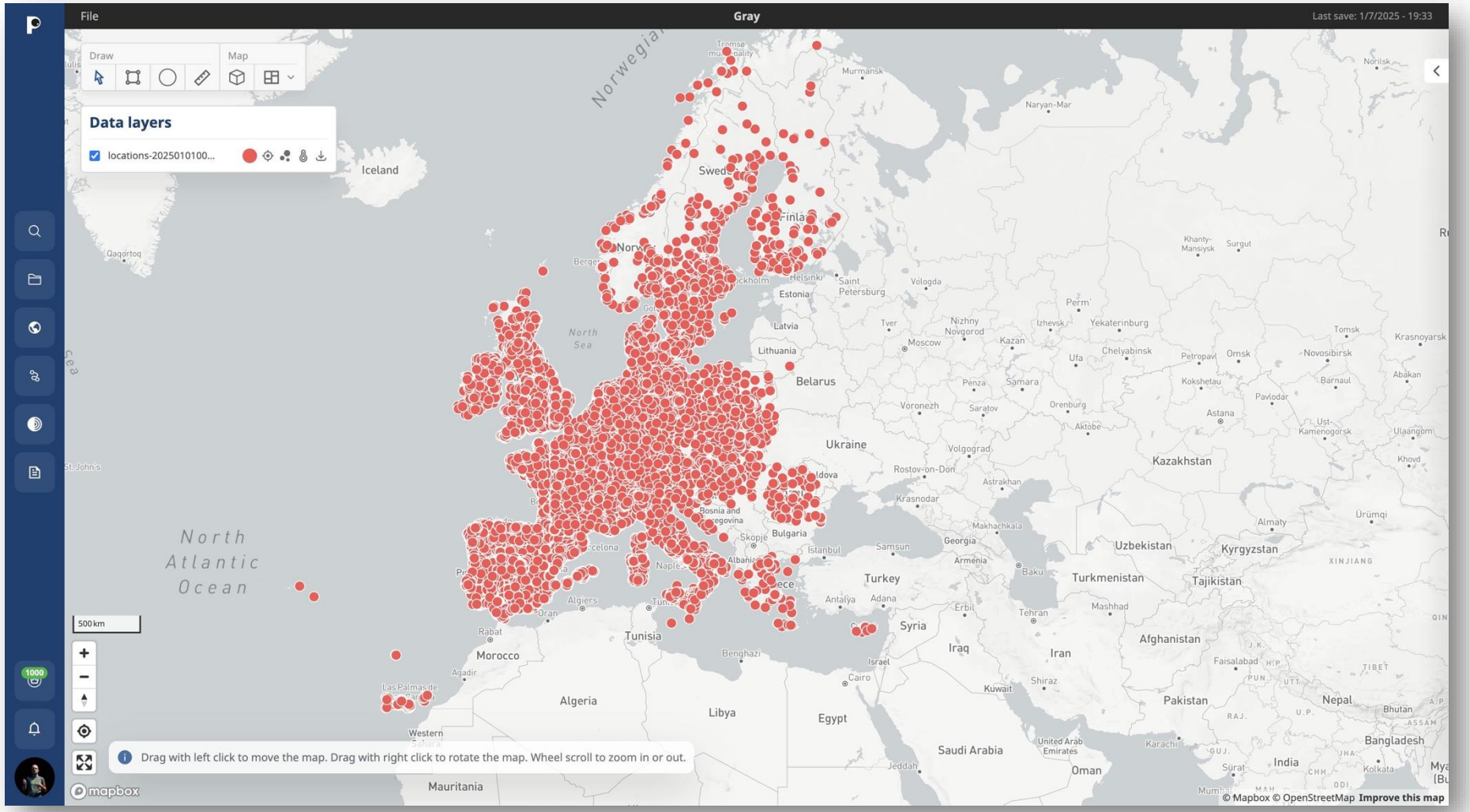
Unacast's Data Linkages enables you to bridge the identity gap by seamlessly connecting MAIDs to hashed emails (HEMs) and IPs.

**intuitive. Another thing is it offers that psychographic segmentation right in the app. At a quick glance,**

posted shows that most of the data consists of unlinked data elem

cannot be associated with any device. Even when a MAID is linked to location data, associating a specific person with any of this data would demand significantly more processing and supplementary datasets. The potential for tracking or profiling any person with this data is further limited by the restricted time span it covers. Harm is unlikely as a direct result of this incident.

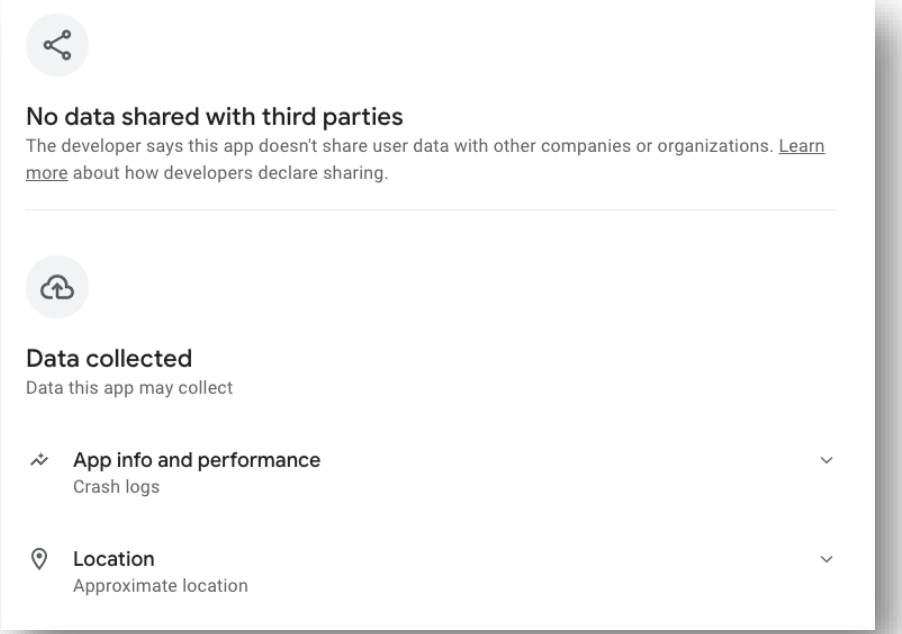
# Gravy Analytics location data breach (2025)



# Where does the data come from?






Source for app IDs in the leaked data

# NRK's experiment: from Funny Weather to Venntel

To try to get to the bottom of this, I started an experiment in February. I installed lots of apps on a spare phone. I would then carry that phone everywhere.

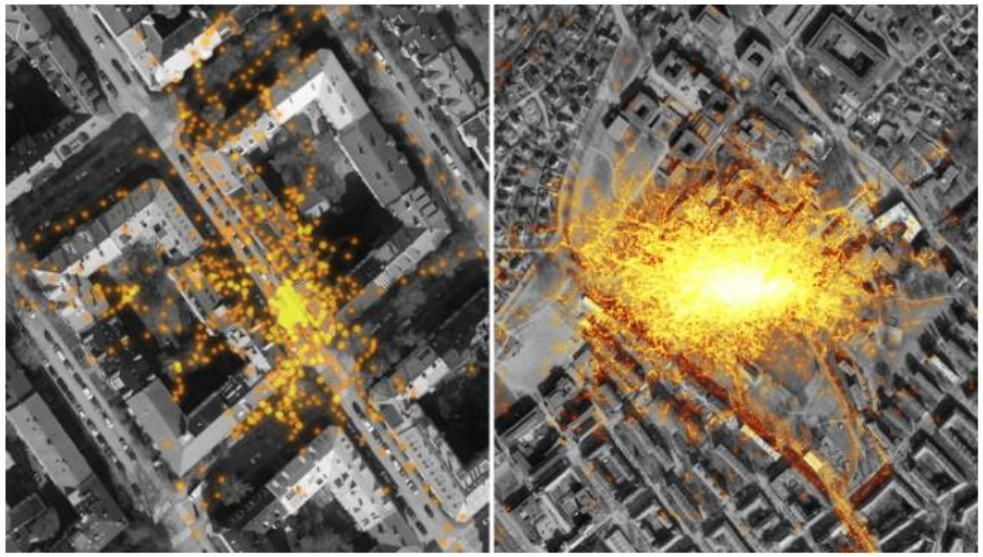
NRK

# NRK's experiment: from Funny Weather to Venntel

## Data for sale

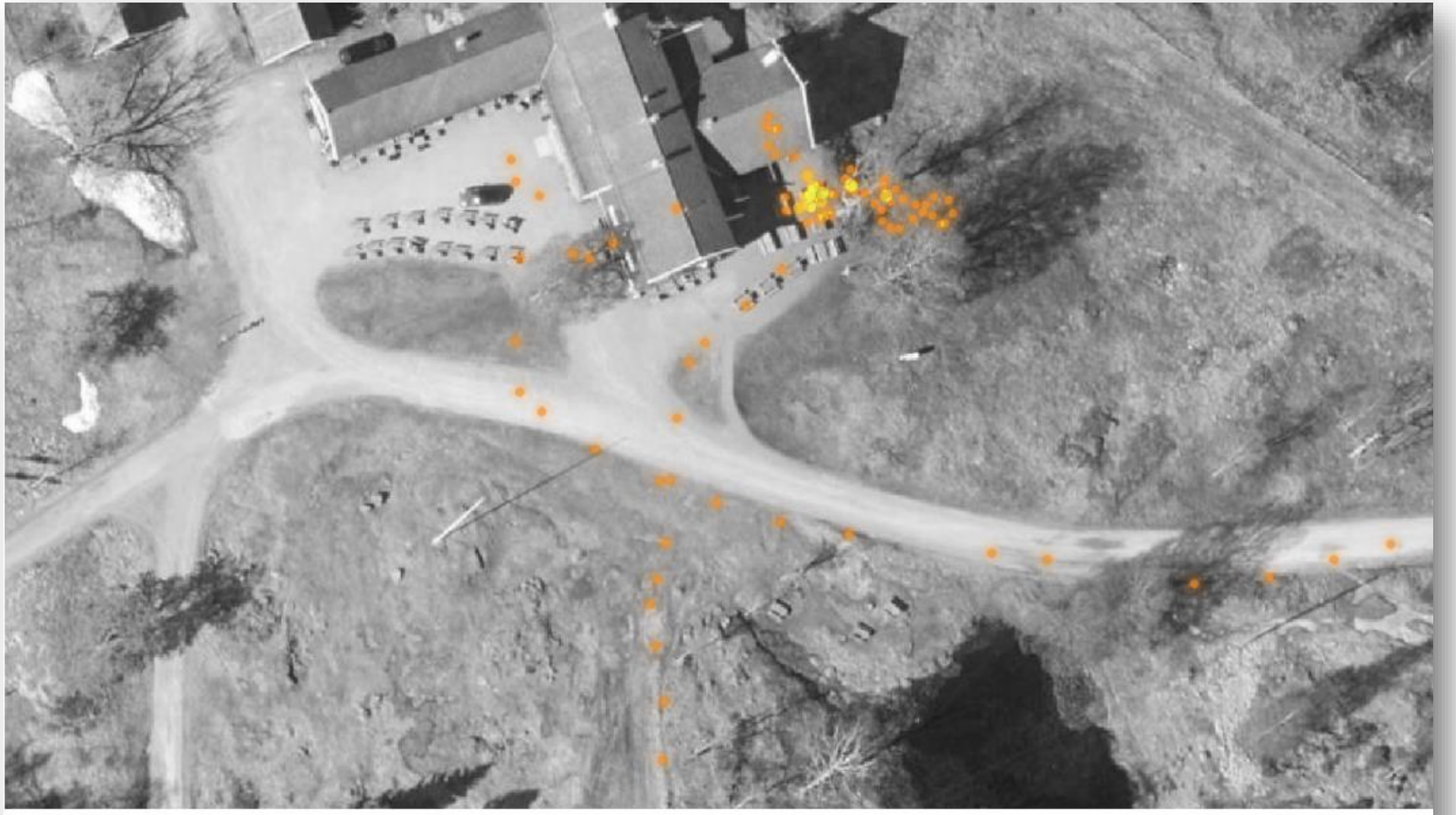
NRK

Almost a month later, I received an interesting email attachment from Venntel. It contained information on where I'd been 75,406 times since 15 February. Suddenly I could retrace my every step – on a hike, out for a drink, and visiting my grandmother in Southern Norway.



DOTS: The left picture shows registrations of my movements in the area where I live. In the picture to the right, you'll see a map of the NRK headquarters at Marienlyst. Over time, there have been an enormous number of registrations here. Illustration: Harald K. Jansson/Norge i bilder

# NRK's experiment: from Funny Weather to Venntel



A BITE TO EAT: I entered from the path on the right. Then I paused in the main courtyard, slightly confused, before finding a wooden bench to the right. In total, the picture is showing 36 minutes of Sunday 9 August. Illustration: Harald K. Jansson/Norge i bilder

NRK

# NRK's experiment: from Funny Weather to Venntel

# ‘A goldmine of *kompromat* ’

Unique ID: h[redacted]

**Employment**
- Decision maker for Government - National Security

**Most frequent locations**
- Rue de la Loi 200, 1049 Bruxelles
- Av. du Bourget 44, 1130 Bruxelles
- Oncology Centre, Universitair Ziekenhuis, Laarbeeklaan 101 1090 Brussels

More locations 〉

**Home**
- [redacted], Ixelles, Brussels

Most frequent driving routes 〉

CANCER TREATMENT CENTRE

**Financial interest tags**
- Personal Debt
- Bankruptcy
- Gambling (high spender)

More 〉

**Money**

**Psychology affinity**
- Dutiful: low affinity
- Materialistic: high affinity

More 〉

**Ego**

**Lifestyle & health tags**
- Frequent alcohol purchaser
- Menopause
- Panic / anxiety disorder

More 〉

DIVORCE LAWYER'S WEBSITE

**Most frequent devices**
- Galaxy S22 Ultra 5G: SM-S9080
- Windows 11 PC / Chrome
- Samsung TV Tizen 6.0

More 〉

**Frequent web visit**
- www.avocat-vdb.be/en/
- www.uzbrussel.be/en/web/oncologisch-centrum/zorgverleners-maagtumor

Web history 〉

**Frequent app use**
- Tinder
- Uber

App history 〉

**Compromise**


Next page 〉

**R**eciprocation

# ‘A goldmine of *kompromat* ’

Audience Profiles > Women > Women in **Menopause** (Cross Pixel)

Clickagy > Partners > Engine Group > Healthcare/Lifestyle > **Cancer** Sufferers/Information Seekers

Epsilon: Household > **Caregiver for** Elderly in Household

Audiences by Skimlinks > Affinity > **Gambling**

Epsilon: Healthcare > Conditions > **Anxiety**

Skydeo > B2B > **Estimated Short Term Debt** > $250K - $500K

Nielsen CPG - Quotient - **Alcohol** - Gin Buyers

TransUnion - Demographics - Marital Status - Likely Recently **Divorced**

Location: Rue de la Loi 200, Brussels
GAID: **12345678-9abc-def0-1234-56789abcdef0**

# ‘A goldmine of *kompromat* ’

CVSS

Base Score

9.6
(Critical)

**Attack Vector (AV)**

Network (N) | Adjacent (A) | Local (L) | Physical (P)

**Attack Complexity (AC)**

Low (L) | High (H)

**Privileges Required (PR)**

None (N) | Low (L) | High (H)

**User Interaction (UI)**

None (N) | Required (R)

**Scope (S)**

Unchanged (U) | Changed (C)

**Confidentiality (C)**

None (N) | Low (L) | High (H)

**Integrity (I)**

None (N) | Low (L) | High (H)

**Availability (A)**

None (N) | Low (L) | High (H)

# Case studies 1 and 2: key takeaways

- Location data *is* sensitive data
- If you can, don't collect it at all; otherwise, minimize collection and use defense in depth
- Threat modeling potential threats to your users (and national security!) posed by ad platforms and third-party SDKs requires:
  - A code- and packet-level audit
  - Imagination!
- How to collect location data while protecting 'sensitive' locations is still an open question

# Case Study 3: Salt Typhoon

# Security and privacy: two pieces of the geopolitical puzzle

| | Attack target: users |
|---|---|
| | Web apps |
| | Userland (native) apps |
| | Operating system |
| | Hypervisor |
| | Firmware |
| | Hardware |
| **Salt Typhoon** | Network |

Insert backdoor here

# It's just IPv6 validation, what could go wrong? (CVE-2023-20273)

```lua
        sub[#sub + 1] = inputTable[i]
      end
    return sub
end

function utils.isIpv4Address(ip)
    if utils.isNilOrEmptyString(ip) then
        return false
    end
    local a,b,c,d=ip:match("^(%d%d?%d?)%.(%d%d?%d?)%.(%d%d?%d?)%.(%d%d?%d?)$")
    a=tonumber(a)
    b=tonumber(b)
    c=tonumber(c)
    d=tonumber(d)
    if not a or not b or not c or not d then
        return false
    end
    if a<0 or 255<a or b<0 or 255<b or c<0 or 255<c or d<0 or 255<d then
        return false
    end
    return true
end

function utils.isIpv6Address(ip)
    if utils.isNilOrEmptyString(ip) then
        return false
    end
    local chunks = utils.splitString(ip,":")
    if #chunks > 8 or #chunks < 3 then
        return false
    end
    for i=1,#chunks do
        if chunks[i] ~="" and chunks[i]:match("([a-fA-F0-9]*)") == nil and tonumber(chunks[i],16) <= 65535 then
            return false
        end
    end
    return true
end

function utils.getInterfaceShortOrLongName(intName)
    if not utils.isNilOrEmptyString(intName) then
        local isIR = utils.getRequestParameters()
        local intType=string.match(intName,"([^/]+)")
        intType = string.lower(intType:sub(1, #intType - 1))
        local slotPos=string.find(intName,"%d")
        local slot=string.sub(intName, slotPos)
        if intType=="te" then
```

```lua
-- CSCwh87343: As a cardinal rule for any validation or check, assumes the input is invalid.
-- Returns true if the ip matches the ipv6 pattern requirement

-- check for ipv6 format, should be 8 'chunks' of hex numbers/letters
-- without leading/trailing chars
-- or fewer than 8 chunks, but with only one `::` group
function utils.isIpv6Address(ip)
    -- Check if the input is a string
    if utils.isNilOrEmptyString(ip) or type(ip) ~= "string" then
        return false
    end

    -- check for ipv6 character format
    local addr = ip:match("^([a-fA-F0-9:]+)$")

    -- address part
    if addr ~= nil and #addr > 1 then
        -- chunk count, double colon
        local nc, dc = 0, false

        -- Process each colon separated chunk iteratively, take each chunk text and the number colons
        for chunk, colons in addr:gmatch("([^:]*)(:*)") do
            -- max allowed chunks, 7 if there is a double chunk, 8 otherwise
            if nc > (dc and 7 or 8) then return false end

            -- chunk hex value check
            if #chunk > 0 and tonumber(chunk, 16) > 65535 then
                return false
            end

            if #colons > 0 then
                -- max consecutive colons allowed: 2
                if #colons > 2 then return false end
                -- double colon shall appear only once
                if #colons == 2 and dc == true then return false end
                -- If there is a double colon and we haven't seen one yet, mark that we are seeing one
                if #colons == 2 and dc == false then dc = true end
            end
            nc = nc + 1
        end
        return true
    end

    return false
end
```

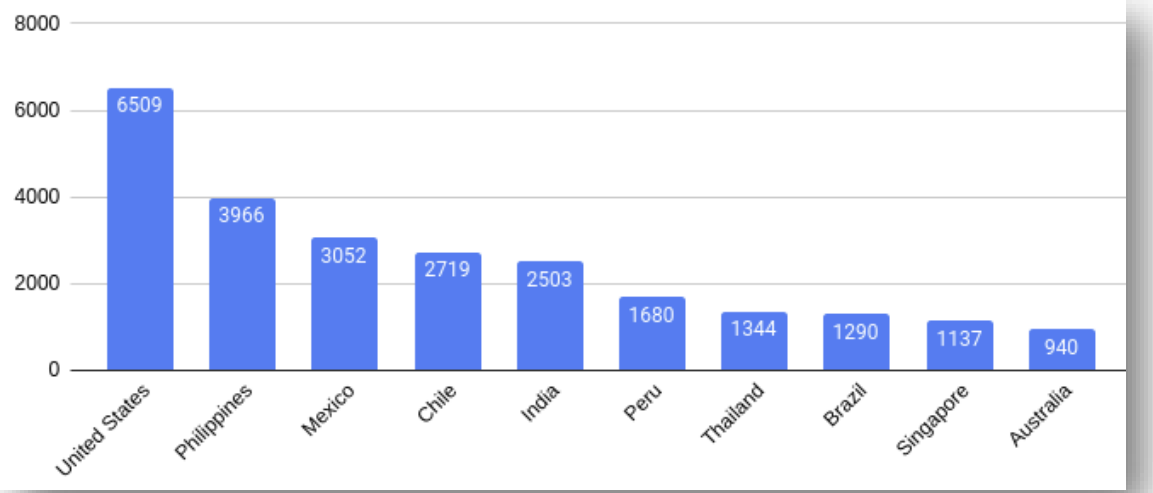
```
lua isIpv6Address.lua '2001:db8:3333:4444:5555:6666:7777: ; ls'
true
```

# CVE-2023-20198 and CVE-2023-20273 meet telecoms providers

Sept 28th 2023: Cisco support case opened for suspicious behavior on customer device

Oct 16th 2023: Cisco releases critical threat advisory

Oct 18th 2023: >40k devices backdoored (Censys)




# China backdoors the US government's backdoor



Public Law 103-414
103d Congress

An Act

To amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes.

Oct. 25, 1994
[H.R. 4922]

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

## TITLE I—INTERCEPTION OF DIGITAL AND OTHER COMMUNICATIONS

Communications Assistance for Law Enforcement Act.

**SEC. 101. SHORT TITLE.**

47 USC 1001 note.

This title may be cited as the "Communications Assistance for Law Enforcement Act".

**SEC. 102. DEFINITIONS.**

47 USC 1001.

For purposes of this title—

(1) The terms defined in section 2510 of title 18, United States Code, have, respectively, the meanings stated in that section.

(2) The term "call-identifying information" means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.

(3) The term "Commission" means the Federal Communications Commission.

(4) The term "electronic messaging services" means software-based services that enable the sharing of data, images, sound, writing, or other information among computing devices controlled by the senders or recipients of the messages.

(5) The term "government" means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof authorized by law to conduct electronic surveillance.

(6) The term "information services"—

(A) means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and

(B) includes—

# China backdoors the US government's backdoor

*We've created a master key that opens all our country's networks. I'm reminded of the phrase, "Never forge a sword so powerful you wouldn't give it to your worst enemy." China now has that sword.*

~ Jon Pelsen in The Diplomat

# China backdoors the US government's backdoor

*With the exception of how effectively the threat actors executed the campaign at scale,* ***nothing here was significantly novel****...The adversaries in this operation travelled interconnected networks, took advantage of inadequate defenses and monitoring, broke into vulnerable edge devices, and made configuration changes to maintain persistence—****risks that have been well understood by all industries for decades****.*

~ Marc Rogers to the Atlantic Council's Cyber Statecraft Initiative

# China backdoors the US government's backdoor

*Highly targeted individuals should assume that all communications between mobile devices—including government and personal devices—and internet services are at risk of interception or manipulation.*

~ CISA, December 2024

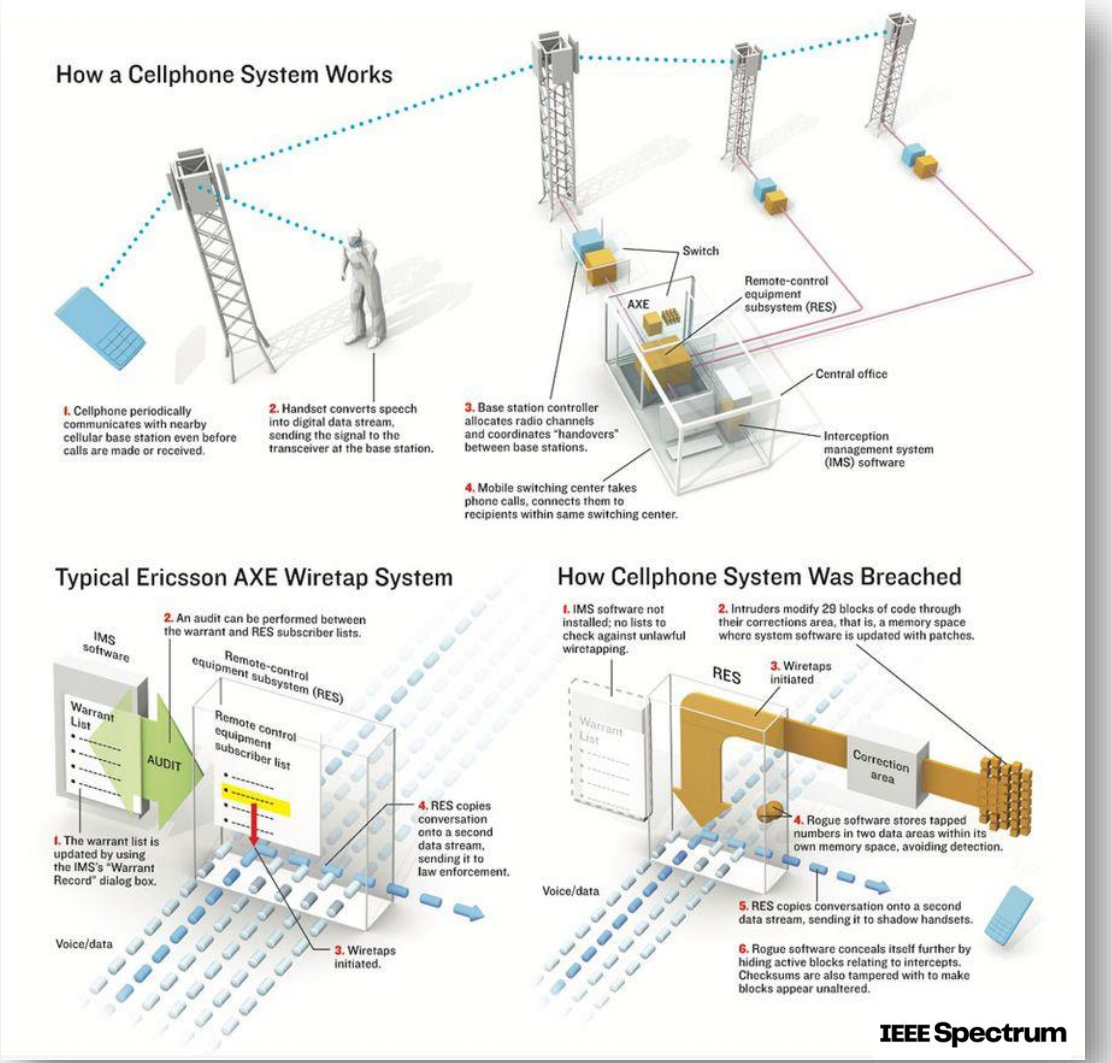
# What did they do?

- Intercepted communications of senior officials within both 2024 presidential campaigns, including texts sent by Trump and Vance
- Monitored US government requests to intercept data, revealing suspected spies
- (Probably) obtained mass metadata of who called/texted whom to map social networks and track political dissidents
- (Probably) also compromised ISPs to read emails
- (Probably) also stole significant corporate IP and university research

And what they *didn't* do:

- Disrupt or cut off communications

# Precedent: the ‘Athens affair’ (2004)

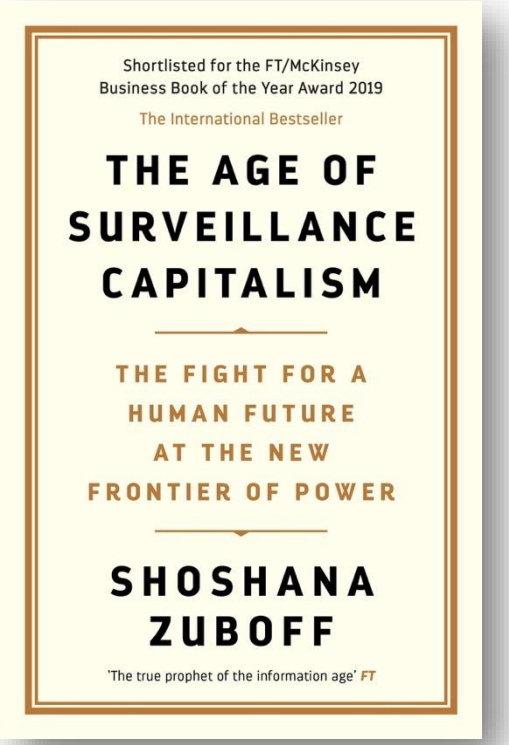


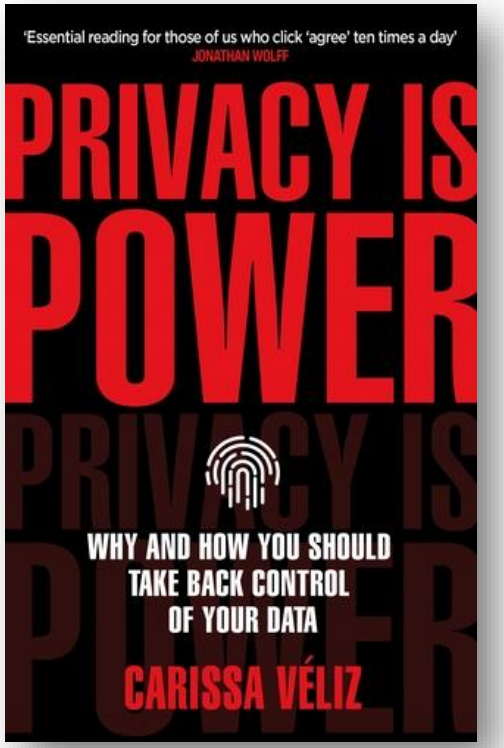
# Case study 3: key takeaways

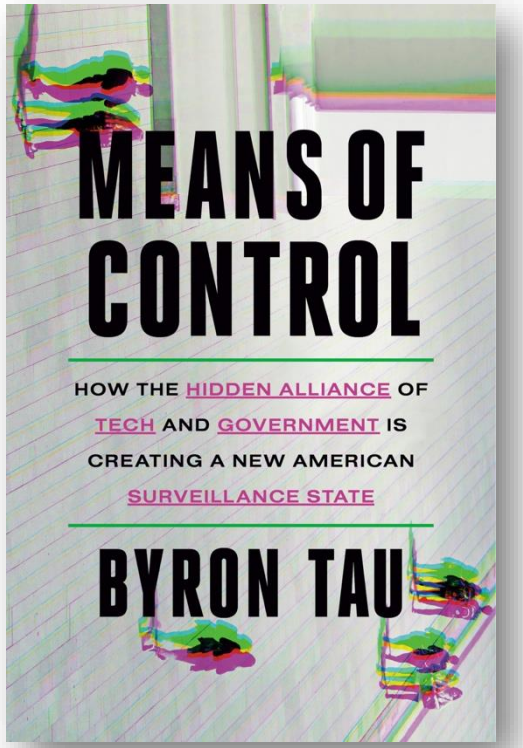
- Our work matters!
- Salt Typhoon is not the first – or the last – threat actor to target lawful interception
- Backdoors will always be high-value targets that are near impossible to protect
  - Security by obscurity will fail
  - Legal/procedural protections will fail
  - Even solid technical protections will likely fail at scale

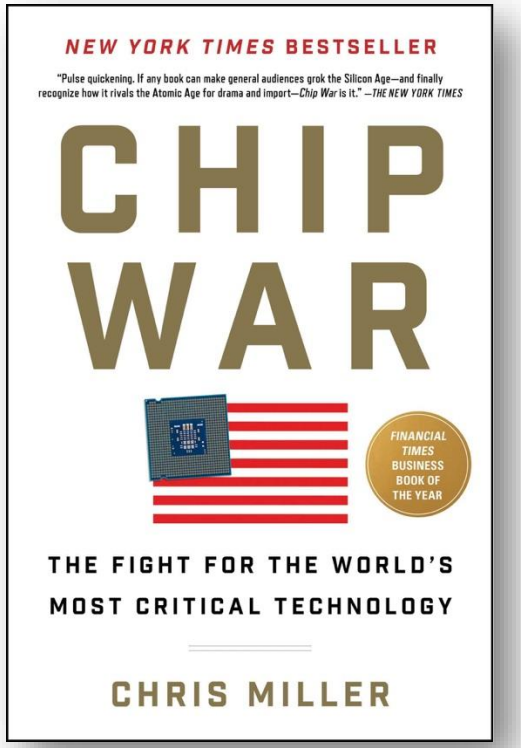
# What next?

# Want to learn more?

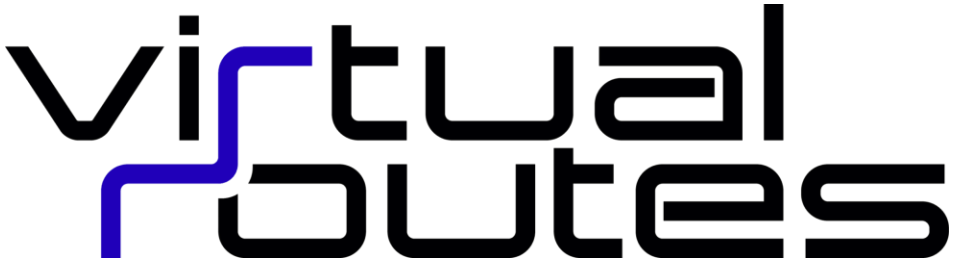


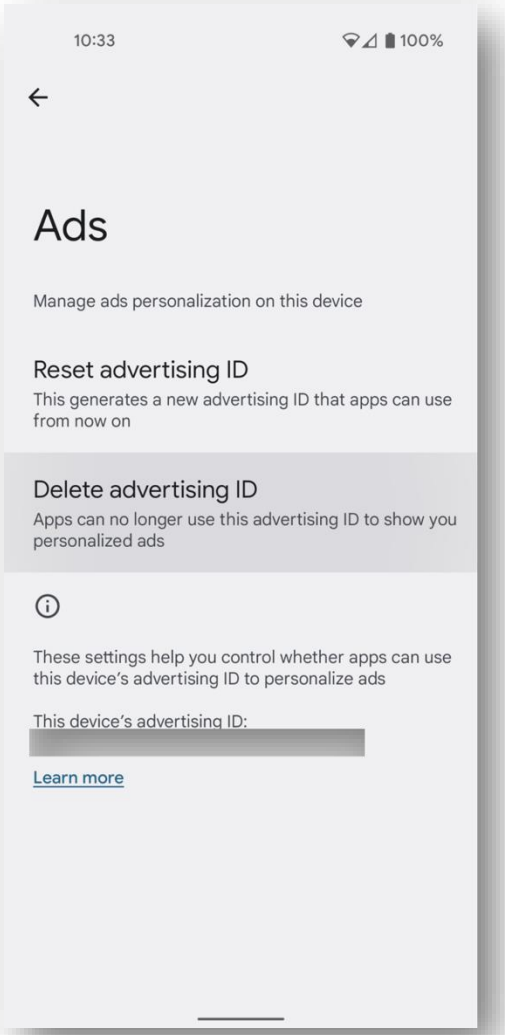



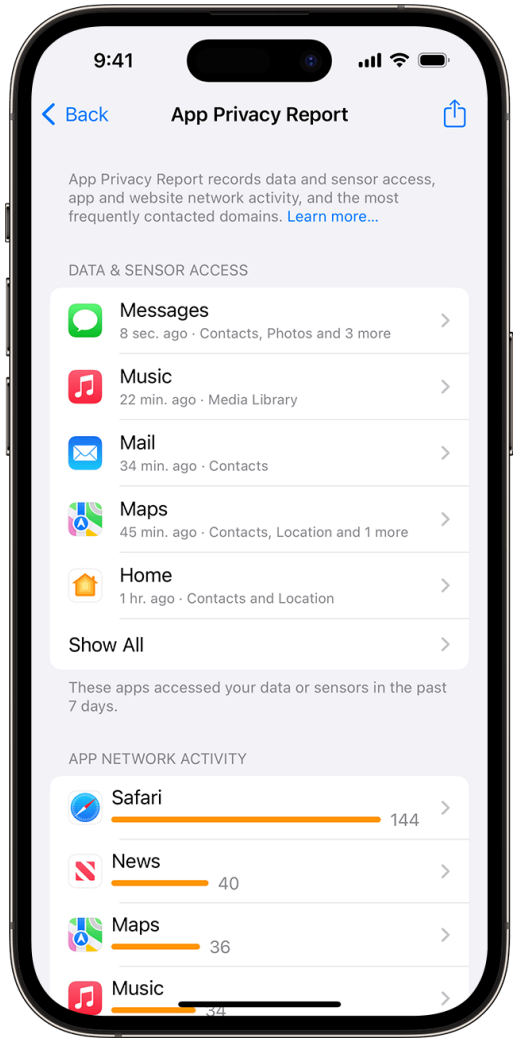
# Want to learn more?

**Thanks for listening!**
**Any questions?**

# P.S. Check your phone!




# Copyright Notice

dynatrace

CLOUD DONE RIGHT