



# Data Access Rights Exploits Under New Privacy Laws

Amber Welch, Privacy  
Technical Lead @ Schellman



Hi,

I'm Amber Welch,  
and I evaluate  
corporate privacy  
programs



# Privacy!

I like XKCD,  
oxford commas,  
and reading  
privacy laws so  
you don't have  
to

## OPINIONS ON INTERNET PRIVACY

### THE PHILOSOPHER:

"PRIVACY" IS AN IMPRACTICAL WAY TO THINK ABOUT DATA IN A DIGITAL WORLD SO UNLIKE THE ONE IN WHICH OUR SOCI-

*SO BORED.*



### THE CRYPTO NUT:

MY DATA IS SAFE BEHIND SIX LAYERS OF SYMMETRIC AND PUBLIC-KEY ALGORITHMS.

WHAT DATA IS IT?

MOSTLY ME EMAILING WITH PEOPLE ABOUT CRYPTOGRAPHY.



### THE CONSPIRACIST:

THESE LEAKS ARE JUST THE TIP OF THE ICEBERG. THERE'S A WAREHOUSE IN UTAH WHERE THE NSA HAS THE *ENTIRE* ICEBERG.

I DON'T KNOW HOW THEY GOT IT THERE.



### THE NIHILIST:

JOKE'S ON THEM, GATHERING ALL THIS DATA ON ME AS IF ANYTHING I DO MEANS ANYTHING.



### THE EXHIBITIONIST:

MMMM? I SURE HOPE THE NSA ISN'T WATCHING ME BITE INTO THESE JUICY STRAWBERRIES!!

OOOPS, I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.

GOOGLE, ARE YOU THERE?

GOOGLE, THIS LOTION FEELS SOOOO GOOD.



### THE SAGE:

I DON'T KNOW OR CARE WHAT DATA *ANYONE* HAS ABOUT ME.

DATA IS IMAGINARY. THIS BURRITO IS REAL.






# The next 20 minutes...

- Data subject requests
- DSR exploits
- Defense strategies

# Data Subject Requests



AKA: DSRs,  
DSARs, SARs, or  
Consumer Rights

An abstract geometric graphic on the right side of the slide. It features a series of dark gray, three-dimensional rectangular blocks arranged in a stepped, diagonal pattern. Two blocks are highlighted: one is light green and the other is blue, both positioned towards the bottom right of the arrangement.

# Global Data Privacy Era





# GDPR/CCPA Rights

Four key rights to exploit:

- Access
- Rectification/modification (GDPR only)
- Erasure (deletion/forgotten)
- Portability





# New Challenges

- GDPR added indirect identifiers to definition
- California added household and device data
- Both include currently non-personal data that could *potentially* be linked to identifying data
- Google Spain lawsuit: “controllers without control”



# Company Prep (or not)

Mostly unprepared in the US:

- Panic and FUD
- Provide all the data
- See it as a legal issue; outsource to legal firms
- Consider non-compliance a greater risk than a breach of one individual's data

# DSR Exploits





# Legal DDoS

- Bad actors can jump in with legitimate grassroots protest or educational campaigns
- Great time to flood with boilerplate text
- Can distract security and legal teams
- Average UK DSR cost £145
- Outsourcing DSRs to legal firms is expensive

# Legal DDoS

James Titcombe submitted a request that cost **£240,000** for a legal firm to process (1)



# Other Bad Actors

- Privacy/security OSINT
- Guerilla marketing
- Competitor research
- Disgruntled employees
- Lawyers pressuring companies to settle



# Phishing

- Requests for indirect identifiers
- Requesting data for other people with your own name
- Escalating from low-sensitivity requests to confidential data
- Adding household or child data to a successful request

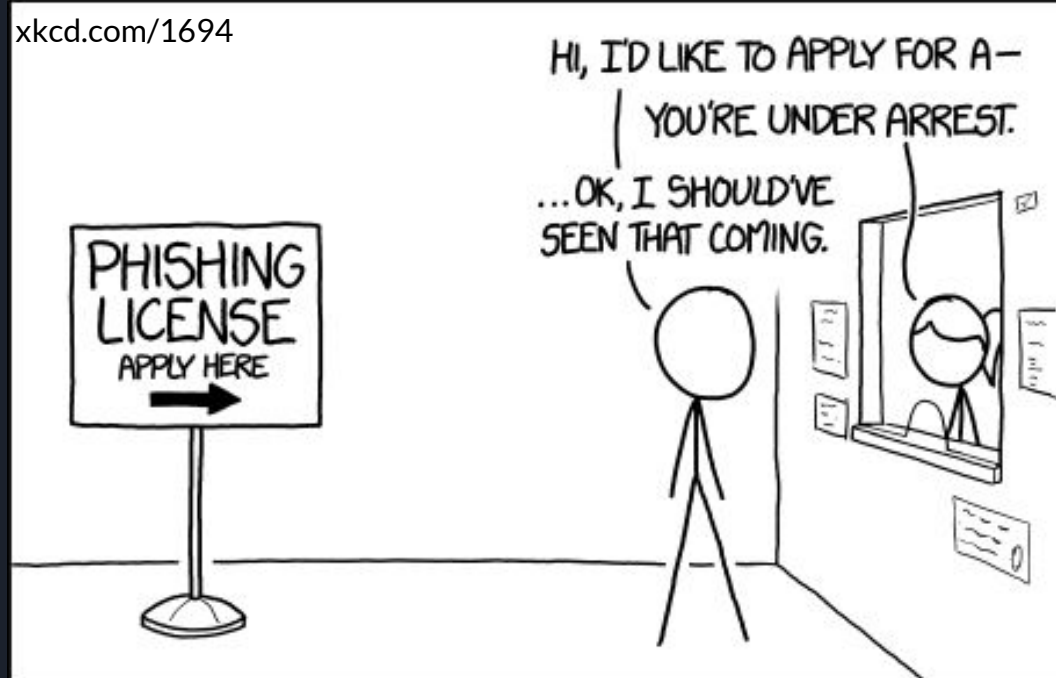
IF YOUR EMAIL ADDRESS IS  
[FIRST INITIAL] + [LAST NAME]  
@GMAIL.COM  
YOU GRADUALLY GET TO KNOW  
LOTS OF OLDER PEOPLE WHO  
HAVE THE SAME NAME PATTERN

YES, I KNOW IT WOULD MAKE  
*SENSE* IF THAT WERE YOUR  
EMAIL ADDRESS, BUT IT'S NOT.



# Social Engineering

- Call pretexting
- Confirming profile data
- Learn new data
- Use for freshly breached data





# Evaluating a Target

- Vague or old public privacy policy
- DPO-for-hire or no executive privacy role
- No named Privacy or Security Officer



# Pribo Assessment Tool

Pribo.org makes alluvial diagrams of public privacy statements. They give a high level estimate of the privacy program maturity.





# Weak Targets

- Companies with a high volume of indirect identifiers without account or name
- International charities
- Social media startups
- SMBs in minimally regulated industries
- Apps without 2FA

# Without 2FA:



**Jean Yang**

@jeanqasaur

Follow



Today I discovered an unfortunate consequence of GDPR: once someone hacks into your account, they can request--and potentially access--all of your data. Whoever hacked into my @spotify account got all of my streaming, song, etc. history simply by requesting it. 🙄

(3)

3:49 AM - 11 Sep 2018



*Subject access rights  
would probably increase  
the incidence of personal  
records being accidentally  
or deliberately opened to  
third parties*

*-Lindop Committee on  
Data Protection, 1978 (2)*

# Defense Strategies





# Common DSR Process

- Request arrives in generic inbox
- Intake team sorts valid/invalid requests
  - If low risk, resolved by support desk
  - If high risk, sent to legal or privacy officer
- Manual processing completed by IT or DBA



# ID Challenges

- Insufficient data to positively link with one person
- Can't require CA consumers to have an account
- Can't collect excessive information for ID purposes
- Can't make the process "burdensome"
- Copies of ID documents are additional sensitive information with low assurance of identity
- GOV.UK Verify service is only 51% successful (4)



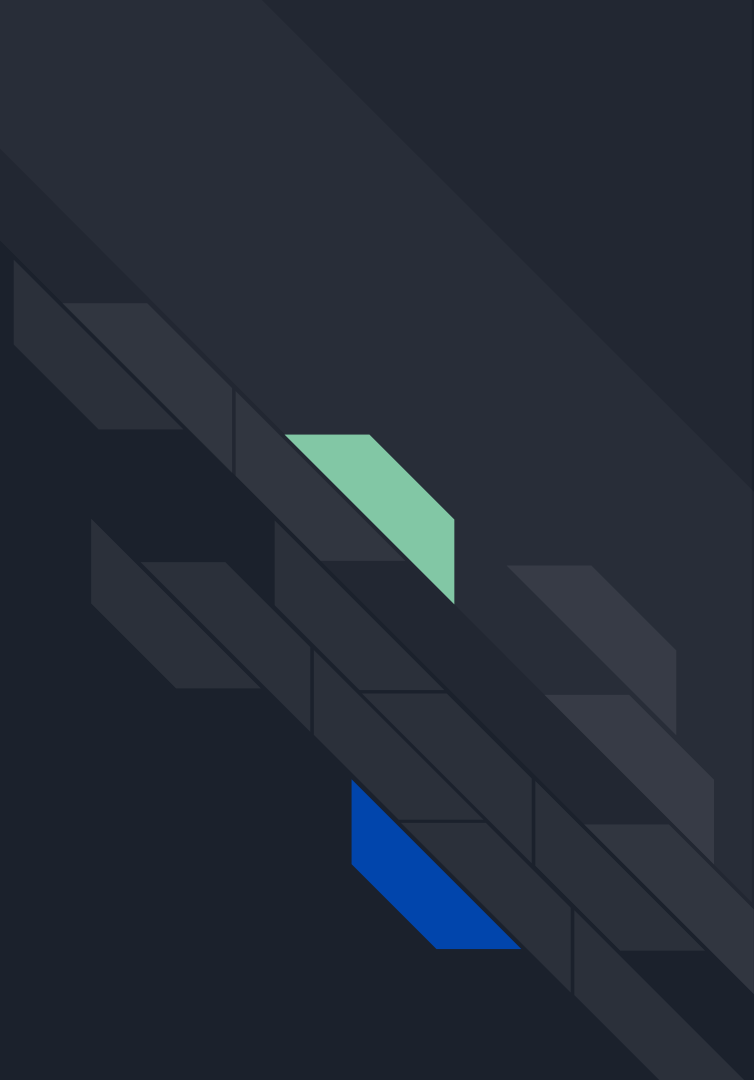


# So What's Safe?

Only two good methods:

- Confirmation from the user of 2+ transactions or activity within the service or application:
  - When did you last stay at our hotel?
  - What are the last 4 digits of the card on file?
- Confirmation of identity as already known by the organization with existing data elements

*You don't need to know  
who the data subject  
actually is, just that it's  
the same individual  
associated with the  
data you hold*



Cat break





# Risk-Based ID Process

- Use graduated ID levels for low- to high-risk data
- Assume ID #s (passport, SSN) are compromised
- Follow NIST digital identity guidelines (5)
- Deny high-risk low-confidence requests



# Minimize Risk

- Use automated self-service when possible
- Add a notice banner to the UI during a pending DSR
- Don't export data the user can already access
- Use secure communications for ID verification
- Campaign for 2FA adoption

# Meet the True Need

Do they just need:

- A password reset?
- Help navigating the app?
- A certain type of data?





# Red Flags

- Requesting a mail copy to a new address
- Common names, especially if merged in deduplication
- Requests based on indirect identifiers
- Requests without an account or activity history
- Requests with multiple associated names
- Frequent similar requests or repeated text
- Unexplained increase in DSR volume

# Default to Denial

Reject all requests until proven valid; legitimate requests can be escalated







# Rejecting Requests

- Repetitive or abusive requests
- Unconfirmed identity
- Data not clearly associated with a confirmed identity
- “Impossible” or requiring “disproportionate effort”
- Adversely affecting the rights and freedoms of others
- Portability requests that are not automated or technically feasible

# Final Thoughts



# Resources

- IAPP, EFF, Nymity, and OneTrust's PrivacyPedia
- Slides and references: [www.github.com/MsAmberWelch/DSR-Exploits](https://www.github.com/MsAmberWelch/DSR-Exploits)
- @MsAmberWelch

I'D LIKE TO THANK MY DIRECTOR,  
MY FRIENDS AND FAMILY, AND—  
OF COURSE—THE WRITHING MASS  
OF GUT BACTERIA INSIDE ME.

I MEAN, THERE'S LIKE ONE OR  
TWO PINTS OF THEM IN HERE;  
THEIR CELLS OUTNUMBER MINE!

ANYWAY, THIS WAS A  
REAL TEAM EFFORT.



xkcd.com/1543



# Sources

1. <https://www.nwemail.co.uk/news/barrow/16447938.nursing-regulator-spent-239000-to-hide-information-on-dalton-dad/>
2. <https://perma.cc/S4J6-HNH4>
3. <https://twitter.com/jeanqasaur/status/1039435801736536064>
4. <https://www.gov.uk/performance/govuk-verify>
5. <https://doi.org/10.6028/NIST.SP.800-63-3>