Data Access Rights Exploits Under New Privacy Laws

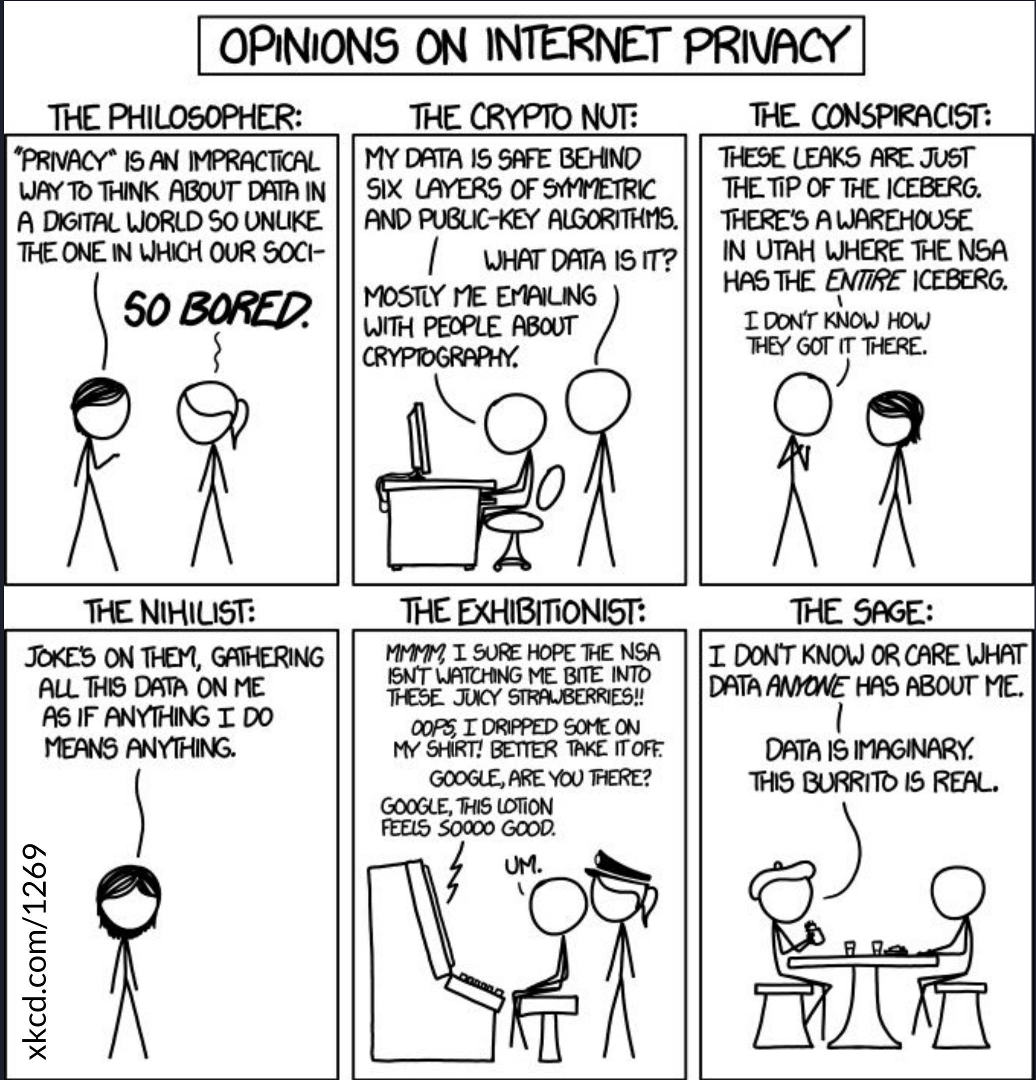
Amber Welch, Privacy Technical Lead @ Schellman

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!!
OOPS, I DRIPPED SOME ON MY SHIRT! BETTER TAKE IT OFF.
GOOGLE, ARE YOU THERE?
GOOGLE, THIS LOTION FEELS SOOOO GOOD.
UM.
THE SAGE:
I DON'T KNOW OR CARE WHAT DATA ANYONE HAS ABOUT ME.
DATA IS IMAGINARY. THIS BURRITO IS REAL.

xkcd.com/1269

The next 20 minutes...

- Data subject requests
- DSR exploits
- Defense strategies

Data Subject Requests

AKA: DSRs, DSARs, SARs, or Consumer Rights

Global Data Privacy Era

Data Access Rights

Four key rights to exploit:

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

Manual vs. Automated

- DSRs can be completed by the user
- Rare DSRs unlikely to be automated
- Different exploits and challenges

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”

Everything can be personal data now

Company Prep (or not)

- 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

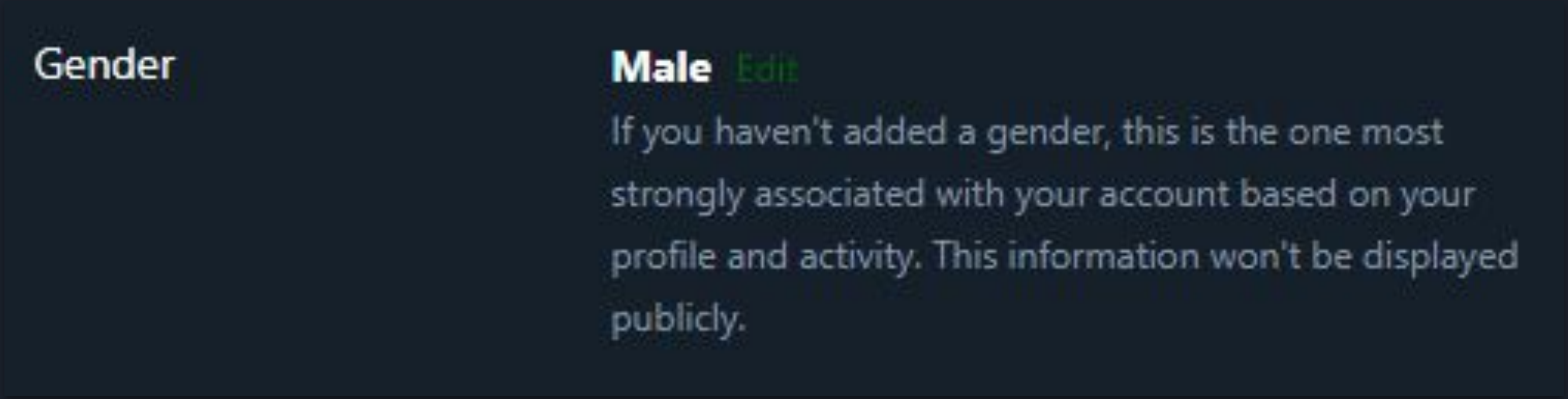
Legal DDoS

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

Legal DDoS

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

Twitter Thinks I'm a Man



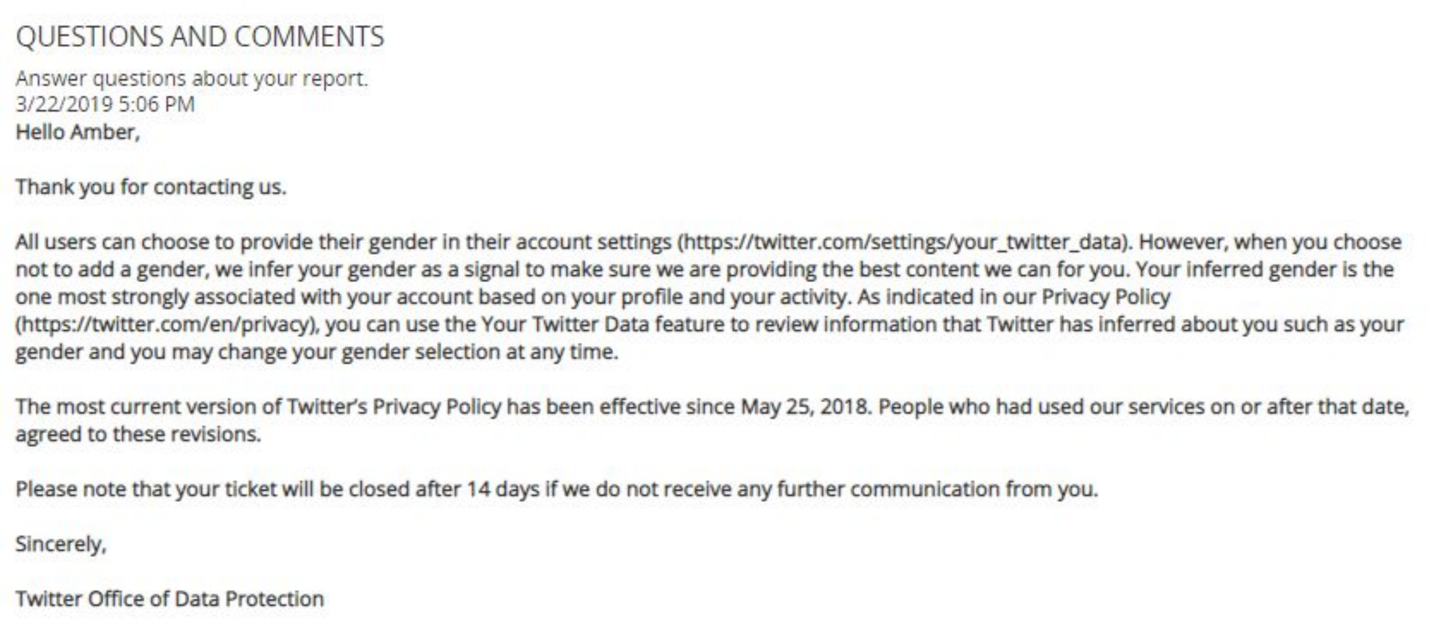
Gender

Male Edit

If you haven't added a gender, this is the one most strongly associated with your account based on your profile and activity. This information won't be displayed publicly.

Let's ask the DPO why!

Twitter Thinks I’m a Man



QUESTIONS AND COMMENTS

Answer questions about your report.
3/22/2019 5:06 PM
Hello Amber,

Thank you for contacting us.

All users can choose to provide their gender in their account settings (https://twitter.com/settings/your_twitter_data). However, when you choose not to add a gender, we infer your gender as a signal to make sure we are providing the best content we can for you. Your inferred gender is the one most strongly associated with your account based on your profile and your activity. As indicated in our Privacy Policy (https://twitter.com/en/privacy), you can use the Your Twitter Data feature to review information that Twitter has inferred about you such as your gender and you may change your gender selection at any time.

The most current version of Twitter’s Privacy Policy has been effective since May 25, 2018. People who had used our services on or after that date, agreed to these revisions.

Please note that your ticket will be closed after 14 days if we do not receive any further communication from you.

Sincerely,

Twitter Office of Data Protection

They paid a lawyer to write this^

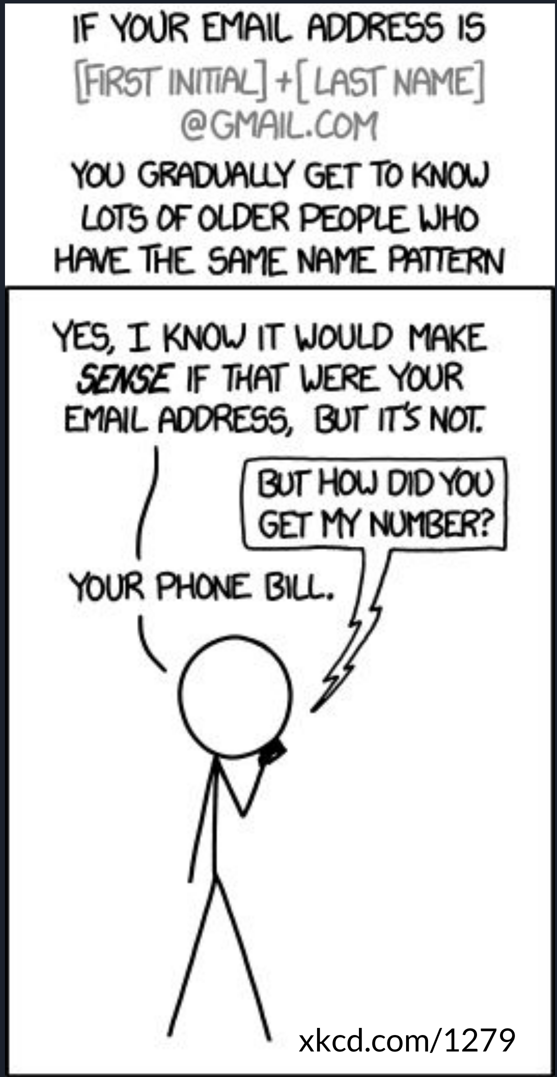
Other Bad Actors

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

Phishing

“What’s in a name?”

-Shakespeare, security researcher


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.
BUT HOW DID YOU GET MY NUMBER?
YOUR PHONE BILL.

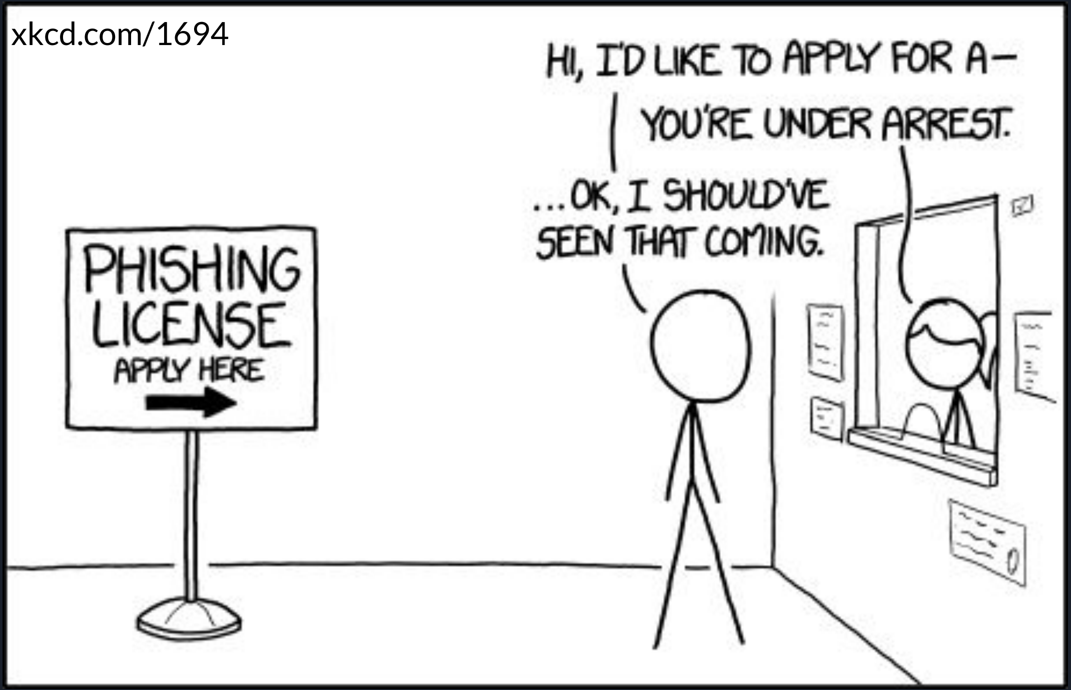
xkcd.com/1279

Phishing Tactics

- Make several requests under common names
- Ask for status updates or the Privacy Officer
- Refuse to narrow the request scope
- Insist you no longer have access to the email
- Offer to confirm ID with other data you have

Social Engineering

AKA, phishing for extroverts



xkcd.com/1694

HI, I'D LIKE TO APPLY FOR A—
YOU'RE UNDER ARREST.
...OK, I SHOULD'VE SEEN THAT COMING.
PHISHING LICENSE
APPLY HERE

Social Engineering

Verbal DSRs:

- Confirm profile data
- Match users across data sets
- Learn new data
- Leverage public or freshly breached data

Social Engineering

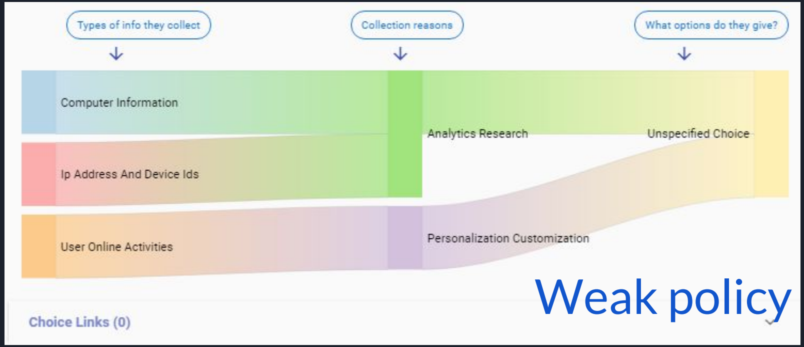
- Encourage the EU citizen myth
- Use clean grammar
- Reference a LinkedIn name with “privacy”
- Escalate to family names or household data
- Escalate from low risk to sensitive data

Evaluating a Target

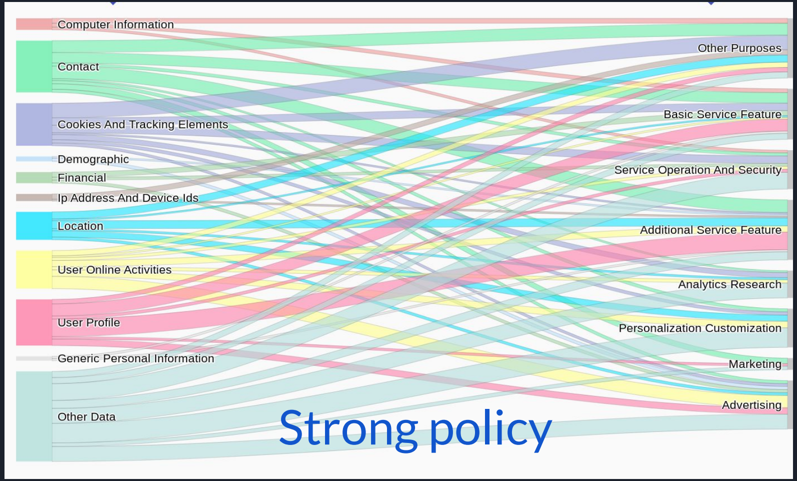
- Vague or old public privacy policy
- DPO-for-hire or no executive privacy role
- No named Privacy or Security Officer

Pribot Assessment Tool

Pribot.org makes alluvial diagrams of public privacy statements to estimate privacy program maturity.



Weak policy

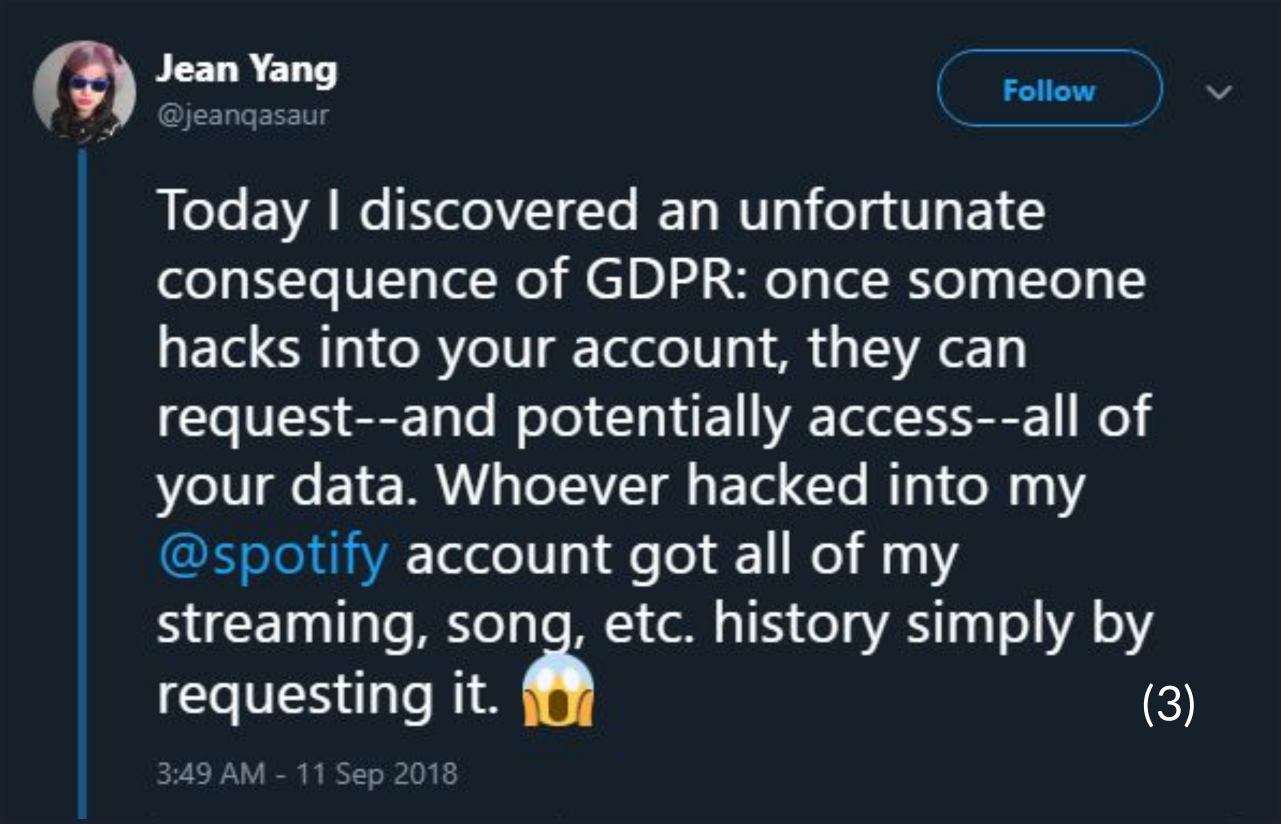


Strong policy

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:



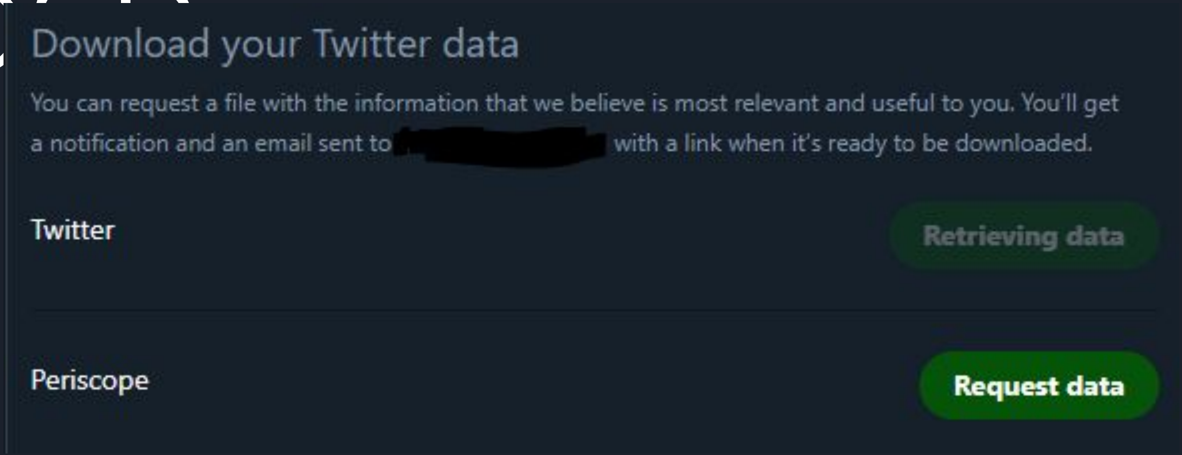
Jean Yang
@jeanqasaur

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. 😱

3:49 AM - 11 Sep 2018

(3)

Post-Authentication DSR

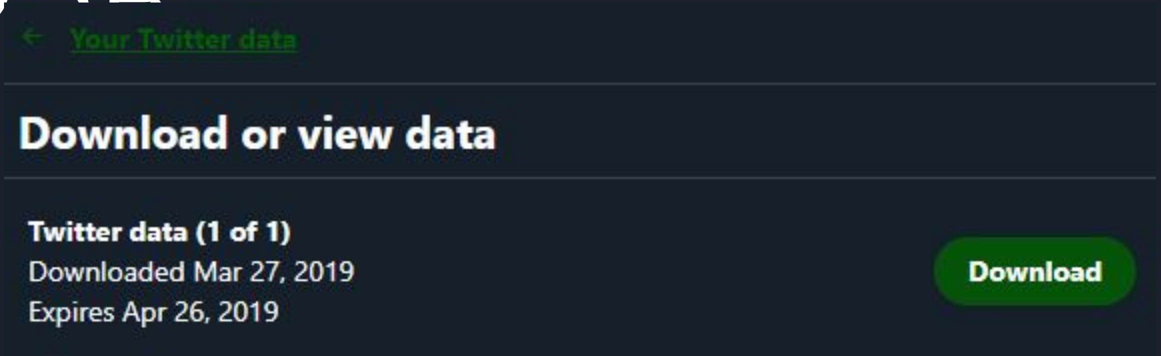


Download your Twitter data

You can request a file with the information that we believe is most relevant and useful to you. You'll get a notification and an email sent to [redacted] with a link when it's ready to be downloaded.

Twitter does not provide a UI banner for the pending DSR and doesn't email until after the data is available

Post-Authentication DSR



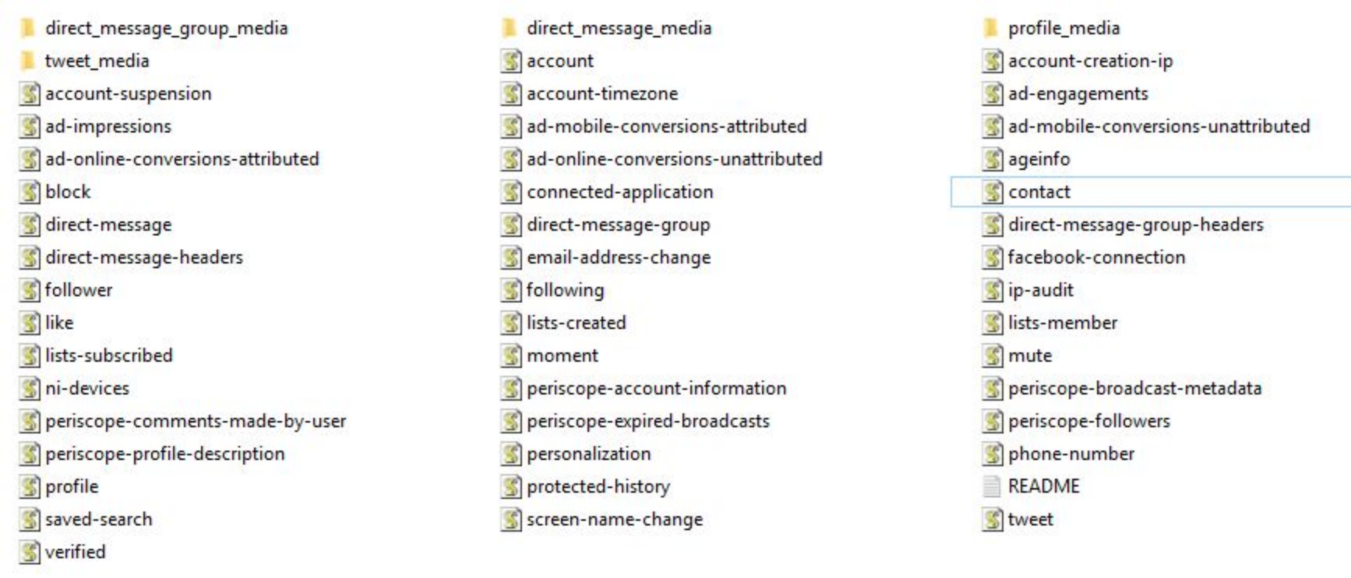
← Your Twitter data

Download or view data

Twitter data (1 of 1)
Downloaded Mar 27, 2019
Expires Apr 26, 2019

No additional 2FA prompt, email notice, or UI banner

Post-Authentication



- direct_message_group_media
- direct_message_media
- profile_media
- tweet_media
- account
- account-creation-ip
- account-suspension
- account-timezone
- ad-engagements
- ad-impressions
- ad-mobile-conversions-attributed
- ad-mobile-conversions-unattributed
- ad-online-conversions-attributed
- ad-online-conversions-unattributed
- ageinfo
- block
- connected-application
- contact
- direct-message
- direct-message-group
- direct-message-group-headers
- direct-message-headers
- email-address-change
- facebook-connection
- follower
- following
- ip-audit
- like
- lists-created
- lists-member
- lists-subscribed
- moment
- mute
- ni-devices
- periscope-account-information
- periscope-broadcast-metadata
- periscope-comments-made-by-user
- periscope-expired-broadcasts
- periscope-followers
- periscope-profile-description
- personalization
- phone-number
- profile
- protected-history
- README
- saved-search
- screen-name-change
- tweet
- verified

This is all the data someone could download many times without the user’s knowledge

> *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

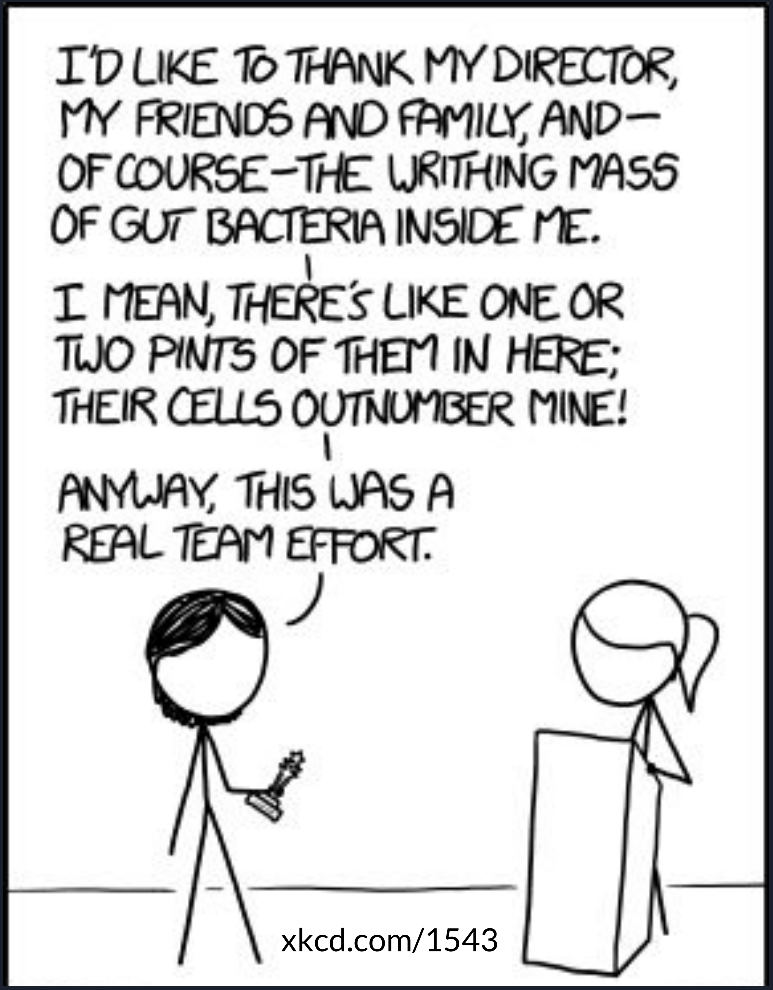
We’re Hiring Pen Testers!

Contact me (@MsAmberWelch) for Junior and Senior pen testing roles:

- Above market pay + bonuses
- 10% 401k match, free healthcare, 5 weeks PTO + holidays
- Certifications, training, and conferences paid
- Mentoring for the junior associate role
- Recognizable clients and supportive team
- No sales/chargeable hours goal or time tracking
- Annual trip to resort w/ plus one (Key West, Cancun, Las Vegas...)

Resources

- IAPP, EFF, Nymity, and OneTrust's PrivacyPedia
- Slides and references: 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