

# Data Access Rights Exploits Under New Privacy Laws

**Amber Welch**  
Privacy Technical Lead, Schellman  
[linkedin.com/in/amberwelch1](https://linkedin.com/in/amberwelch1)  
[github.com/msamberwelch](https://github.com/msamberwelch)  
 @MsAmberWelch

Hi!

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





Today we'll cover:

✓ Data subject  
requests

DSR exploits

✓ Defense  
strategies





# Data Subject Requests





[bit.ly/2DMbzFP](http://bit.ly/2DMbzFP)

# Four exploitable rights

- Access
- Modification (rectification)
- Erasure (deletion/to be forgotten)
- Portability

# New challenges

- Metadata and indirect identifiers
- Household and device data
- Linkable data
- Controllers without control



← Meet Mario Costejo Gonzalez.  
He sued Google Spain.

*What is personal data?*



*Everything*

# Corporate prep (or not)

- Panic and FUD
- Provide all the data
- Outsource to legal firms
- Fear non-compliance more than a breach

Manual  
vs.  
Automated





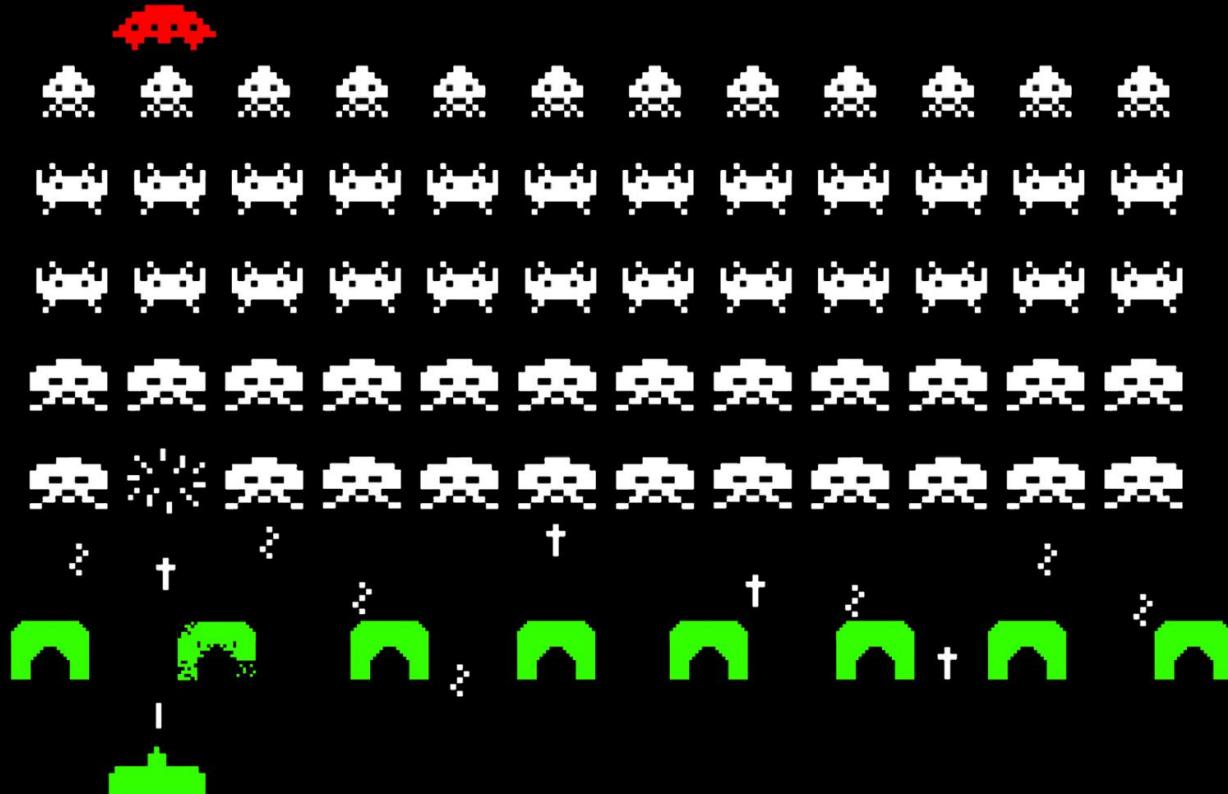
# DSR Exploits



# Legal DDoS

SCORE 1,337

LIVES 



Meet James Titcombe. →  
His DSR cost £240,000.



Twitter thinks I'm a man.  
Let's ask the DPO why!

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.

# Twitter paid a lawyer to write this.

## 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](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

SHIP YOUR ENEMIES



Do you hate your Insurance Provider?

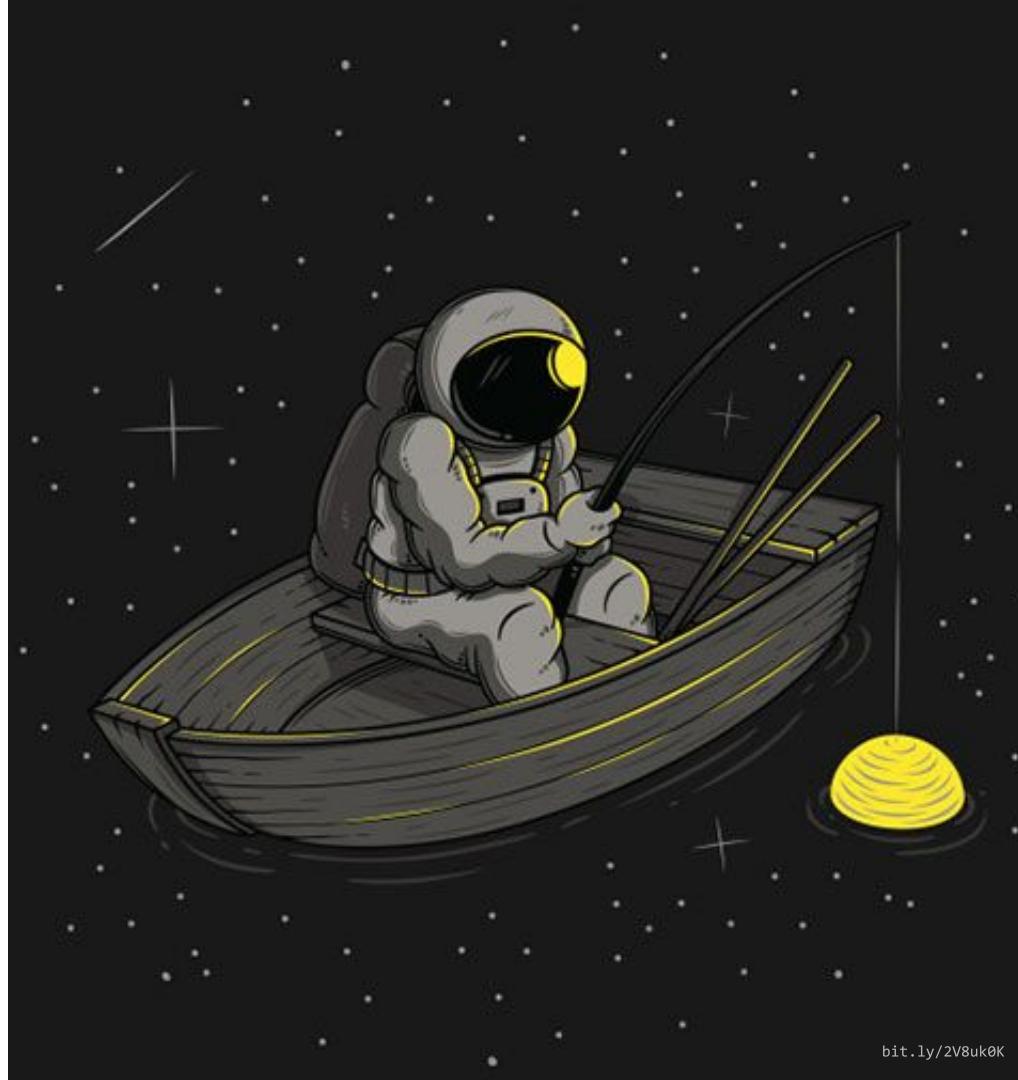
We'll help you send them a GDPR Data Access Request designed to waste as much of their time as possible. They are legally required to respond to your

request within 30 days! 🔥

[www.shipyourenemiesgdpr.com](http://www.shipyourenemiesgdpr.com)

# Phishing tactics

- Ask for updates
- Ask for Privacy Officer
- “I can’t access that email”
- Try to ID with other data
- Escalate with family names
- Escalate to sensitive data
- Use common names



“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.



# Phishing uses

- Confirm profile data
- Match users across datasets
- Learn new data
- Spearfishing and CEO fraud



# Other bad actors

- Guerilla marketing



# Other bad actors

- Guerilla marketing
- Competitor research



# Other bad actors

- Guerilla marketing
- Competitor research
- Disgruntled employees



# Other bad actors

- Guerilla marketing
- Competitor research
- Disgruntled employees
- Lawyers pressuring companies to settle



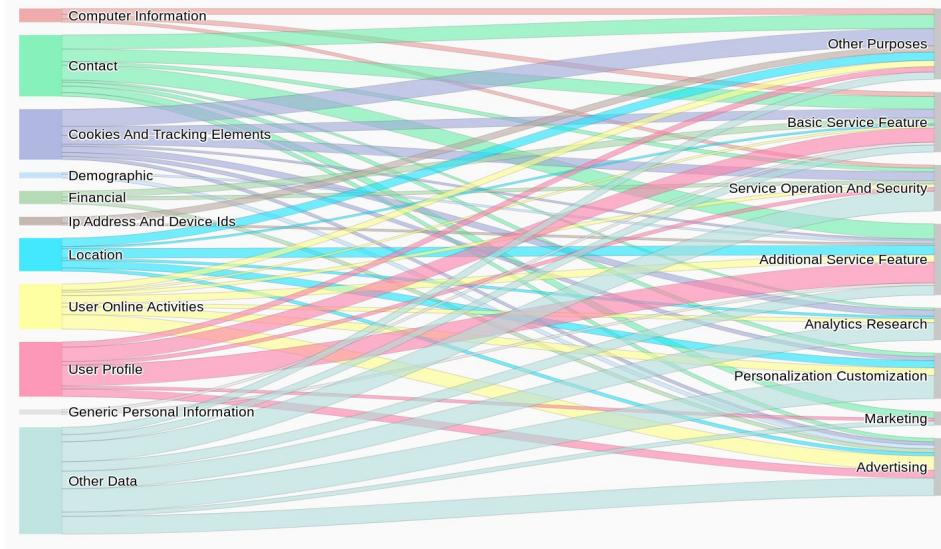
# Other bad actors

- Guerilla marketing
- Competitor research
- Disgruntled employees
- Lawyers pressuring companies to settle
- Intimate partner violence, stalking, and harassment



# Evaluating privacy policies

- Vague or old privacy policy
- No privacy or security officer
- Pribot.org for policy diagram

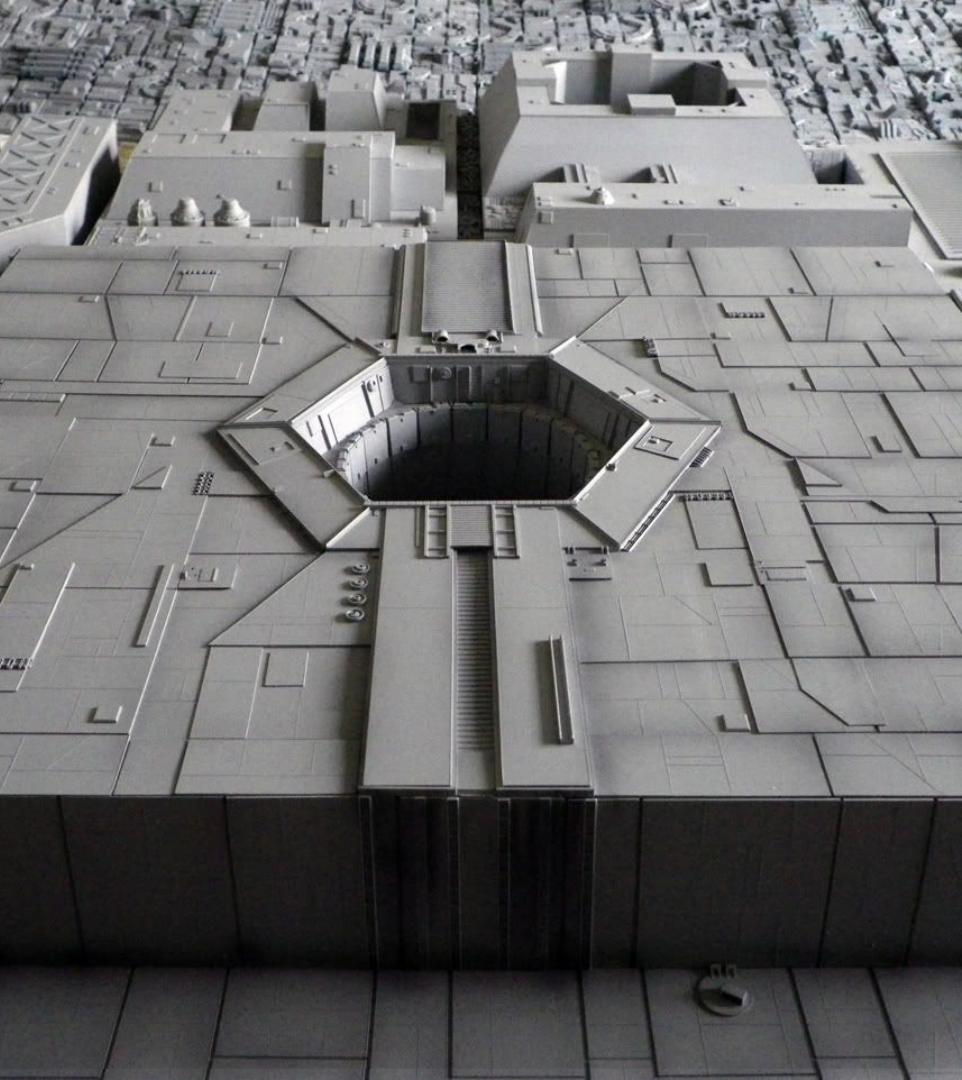


^ Strong policy

< Weak policy

# Weak targets

- Lots of indirect identifiers
- International charities
- Social media startups
- SMBs with minimal regulation
- Apps without 2FA



# Automated DSR without 2FA



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. 🍻

3:49 AM - 11 Sep 2018

# Automated Twitter 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

Retrieving data

Periscope

Request data

Hi Amber Welch, your Twitter data is ready. You have until Apr 27, 2019, 3:53:51 PM to download it before it expires. If you didn't request this information, you can ignore this email.

[Download](#)

[Help](#)

# Twitter data download

← Your Twitter data

## Download or view data

**Twitter data (1 of 1)**

Downloaded Mar 27, 2019

Expires Apr 26, 2019

**Download**

# Twitter data export

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		

“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*





# Defense Strategies



# Three DSR threats

- Invasive identity checks
- Denial of access
- Data breach

# Common DSR process



# ID challenges

- Linking data with one person
- Can't require an account
- Can't collect excessive information
- ID can't be “burdensome”
- GOV.UK Verify is only 51% successful
- ID documents are just extra sensitive information



You don't need to see his identification

# Only two good ID methods

- Confirm ID as already known by the organization
- Confirm 2+ transactions:
  - When did you last stay at our hotel?
  - What are the last 4 digits of the card on file?



[bit.ly/2Vcd5LX](http://bit.ly/2Vcd5LX) | [bit.ly/2pjH8PK](http://bit.ly/2pjH8PK)



# Manual DSRs

- Graduated ID requirements
- Assume ID #s are compromised
- Secure transfers
- NIST Digital Identity Guidelines (SP 800-63)

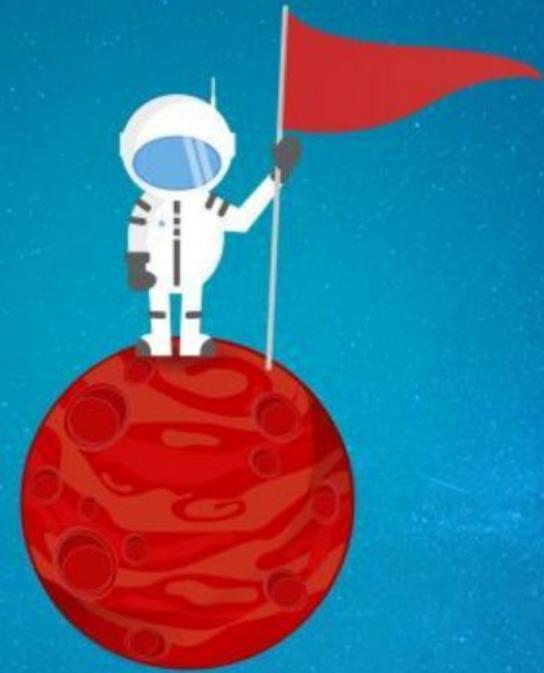


# Automated DSRs

- Re-authenticate the session
- Pending DSR UI banner
- Email notifications
- Campaign for 2FA

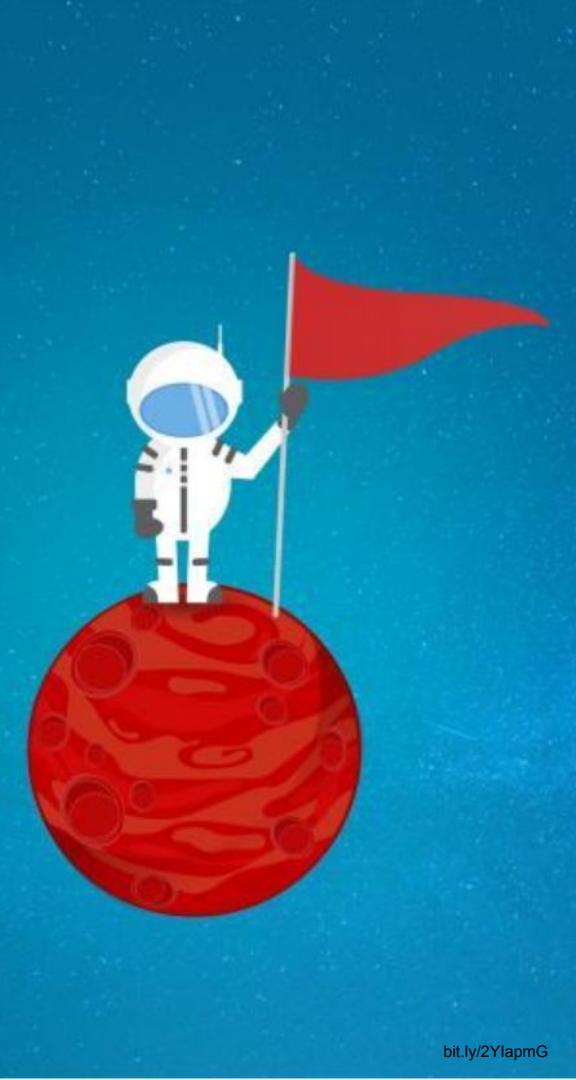
# Red flags

- Requesting a mail copy to a new address



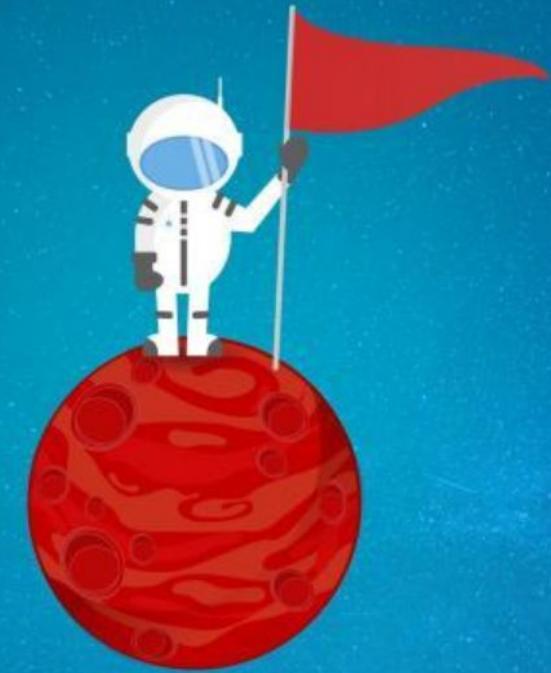
# Red flags

- Requesting a mail copy to a new address
- Common names, especially if deduplicated



# Red flags

- Requesting a mail copy to a new address
- Common names, especially if deduplicated
- Requests based on indirect identifiers



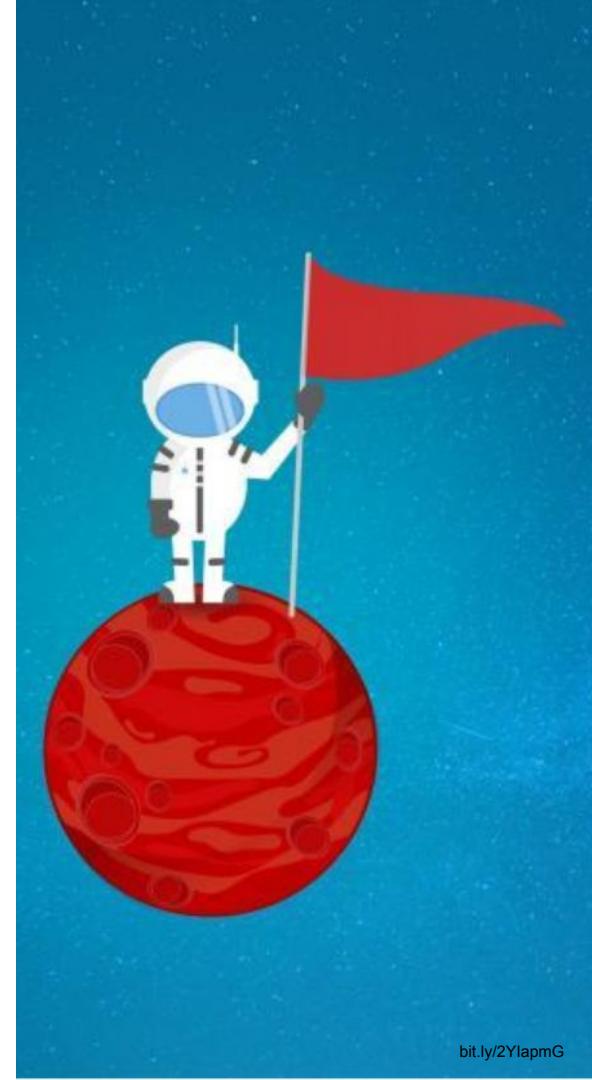
# Red flags

- Requesting a mail copy to a new address
- Common names, especially if deduplicated
- Requests based on indirect identifiers
- Requests without an account or history



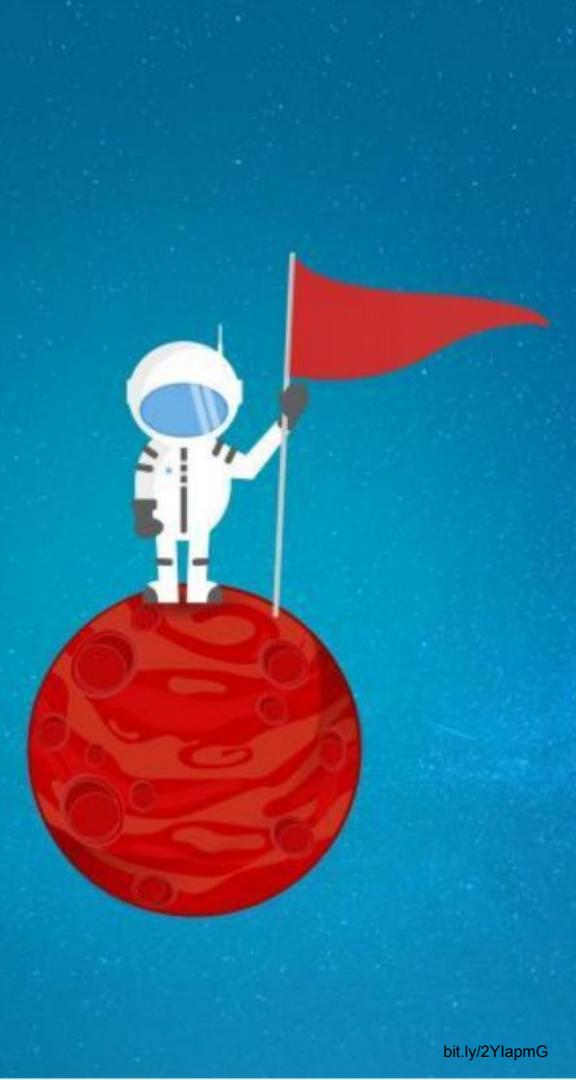
# Red flags

- Requesting a mail copy to a new address
- Common names, especially if deduplicated
- Requests based on indirect identifiers
- Requests without an account or history
- Requests with multiple associated names



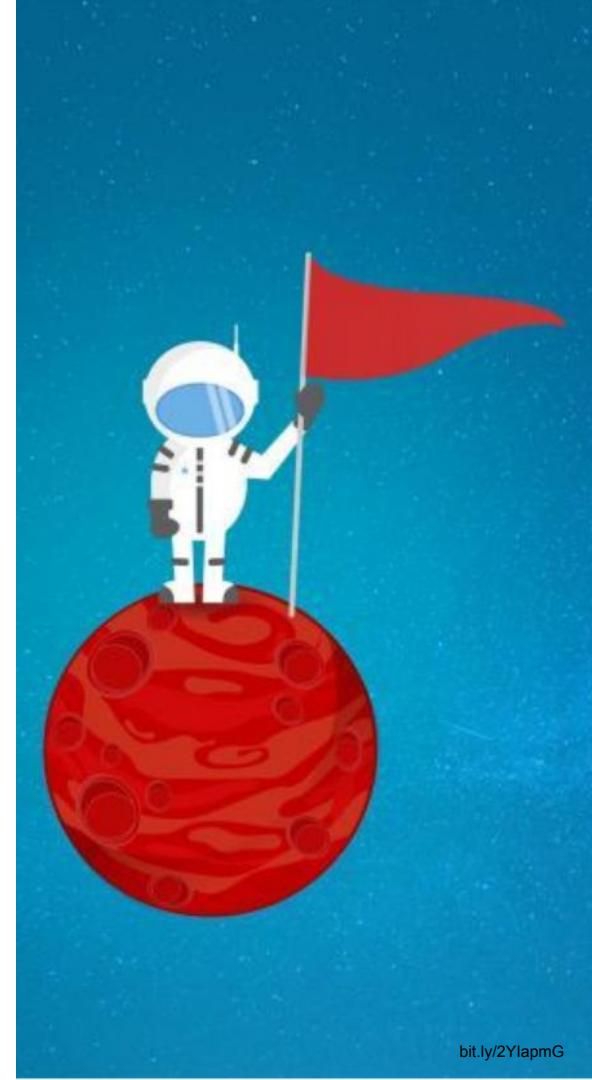
# Red flags

- Requesting a mail copy to a new address
- Common names, especially if deduplicated
- Requests based on indirect identifiers
- Requests without an account or history
- Requests with multiple associated names
- Frequent similar requests or repeated text



# Red flags

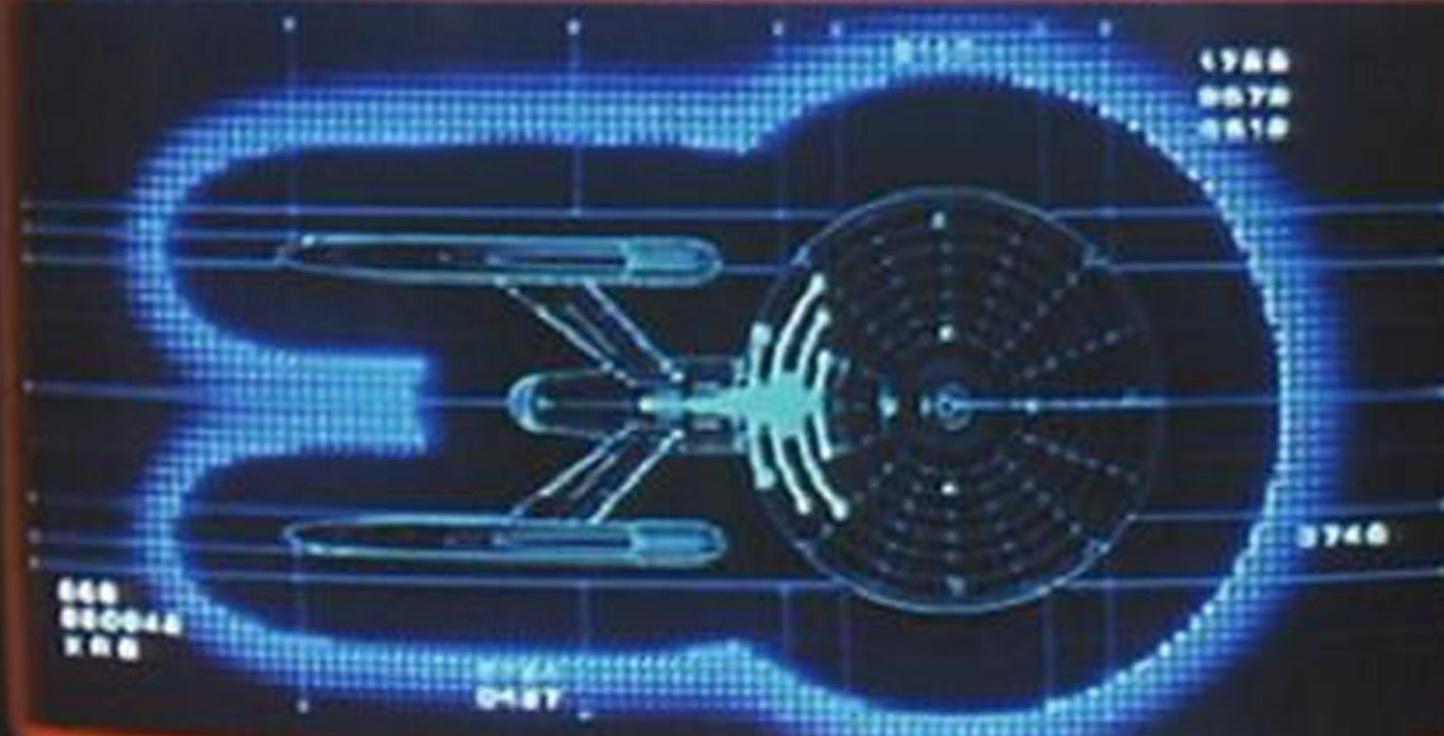
- Requesting a mail copy to a new address
- Common names, especially if deduplicated
- Requests based on indirect identifiers
- Requests without an account or history
- Requests with multiple associated names
- Frequent similar requests or repeated text
- Unexplained increase in DSR volume



# SHIELD STATUS: COMPROMISED

DEFLECTOR POWER

10 30 50 70 90

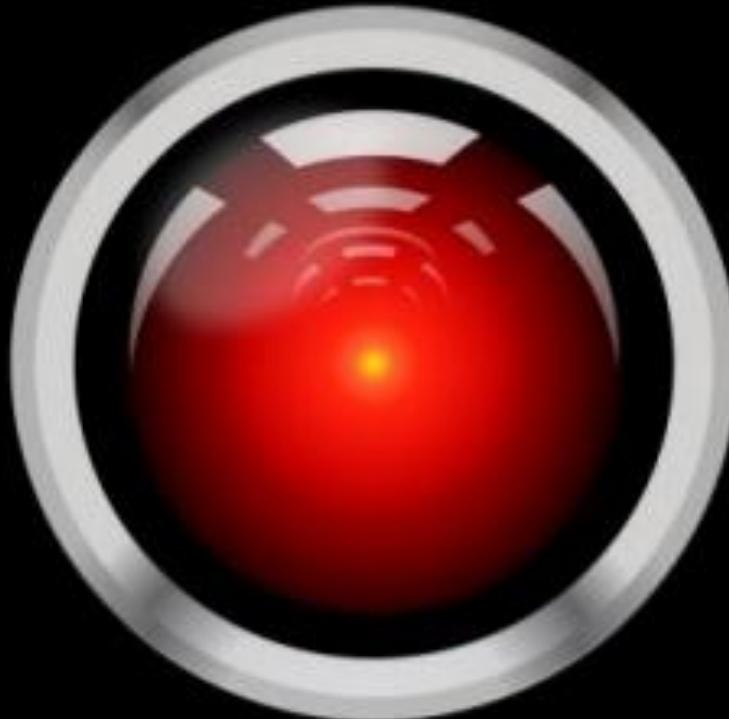


DEFLECTOR STATUS

1181.1

# Cat break





“I'm sorry Dave, I'm afraid I can't do that”

# Rejecting requests

- Repetitive or abusive requests

# Rejecting requests

- Repetitive or abusive requests
- Unconfirmed identity

# Rejecting requests

- Repetitive or abusive requests
- Unconfirmed identity
- Data not clearly associated with a confirmed identity

# Rejecting requests

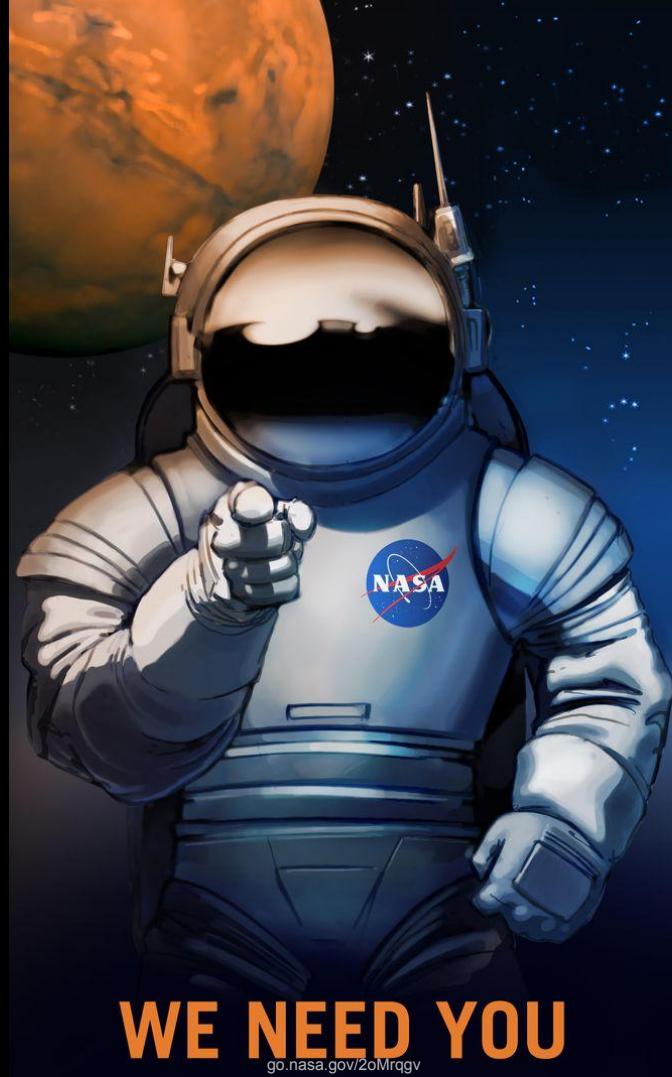
- Repetitive or abusive requests
- Unconfirmed identity
- Data not clearly associated with a confirmed identity
- “Impossible” or requiring “disproportionate effort”

# 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

# 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 not automated or feasible



**WE NEED YOU**

[go.nasa.gov/2oMrqgv](http://go.nasa.gov/2oMrqgv)



## 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-HN4>
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>
6. <https://www.nortonrosefulbright.com/en/knowledge/publications/8f893b33/uk-court-of-appeal-allows-data-subject-access-requests-to-be-made-in-furtherance-of-litigation>
7. <https://hal.inria.fr/hal-02072302/document>



1978

[linkedin.com/in/amberwelch1](https://linkedin.com/in/amberwelch1)

3 [bit.ly/2vzj8uT](https://bit.ly/2vzj8uT) CREDIT 00

Amber Welch

[@MsAmberWelch](https://twitter.com/MsAmberWelch)

[github.com/MsAmberWelch](https://github.com/MsAmberWelch)