LINUXCONFAU

RFC 1984:

Or why you should start worrying about encryption backdoors and mass data collection

Esther Payne

Linux Conf AU 2020

About me

IT Professional with 20 years in Support
e-mail: esther@gladserv.com
LinkedIn: https://www.linkedin.com/in/estherpayne/
twitter: @onepict
mastodon: @onepict@fosstodon.org
telegram: @onepict

Do we need Privacy?

- It's too late my family are all on it.

Do we need Privacy?

- It's too late my family are all on it.
- Even teenagers don't care.

Do we need Privacy?

- It’s too late my family are all on it.
- Even teenagers don’t care.
- Privacy is dead and we don’t need it.

Do we need Privacy?

- It's too late my family are all on it.
- Even teenagers don't care.
- Privacy is dead and we don't need it.
- We need to give up a little privacy for our security.

How to explain Privacy?

Humans learn from stories

OVIDIVS

Ovid and greek myths

- Who was Ovid?

Ovid and greek myths

- Who was Ovid?
- What did he write?

Io and Argus

Io and Argus

Ovid updated the myth

What does this myth have to do with nowadays?

- Branding Argus Panoptes

What does this myth have to do with nowadays?

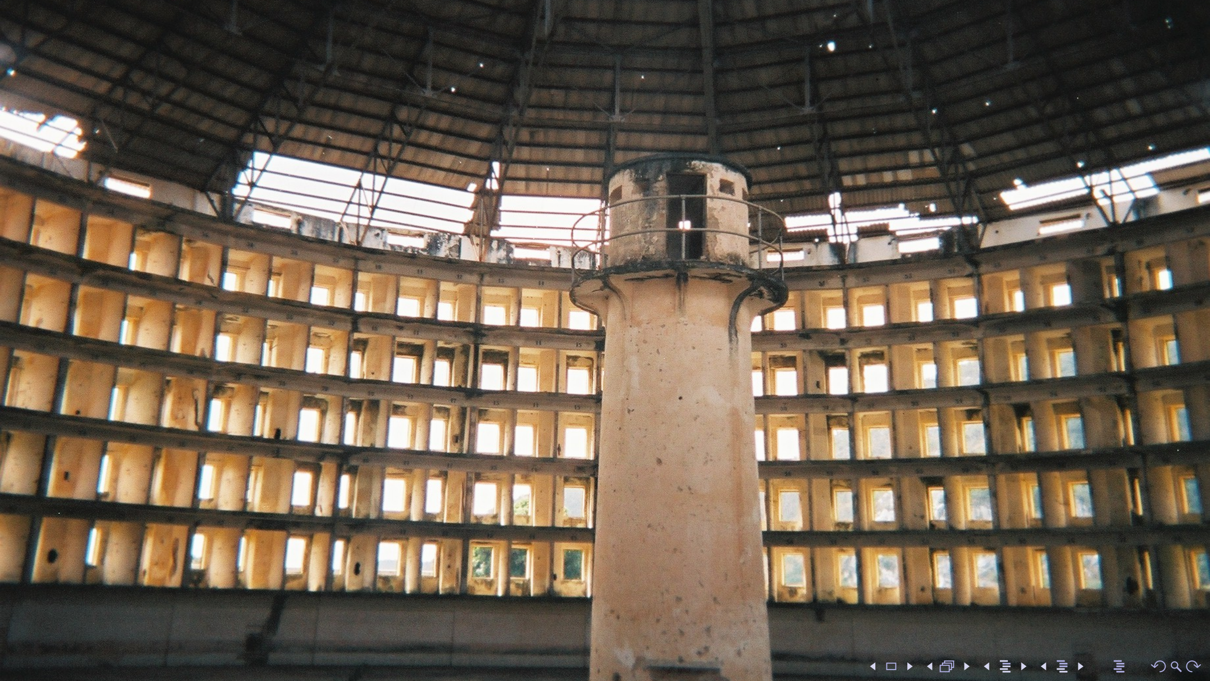
- Branding Argus Panoptes
- We forgot IO DUH!

What does this myth have to do with nowadays?

- Branding Argus Panoptes
- We forgot IO DUH!
- Can we use the myth, or peacocks as a symbol? Is it appropriate?

1984

- George Orwell



1984

- George Orwell
- Again people focus on the tech of oppression.

1984

- George Orwell
- Again people focus on the tech of oppression.
- Need to focus on the why and who.

RFC:1984

- Brian E. Carpenter of IAB and Fred Baker of IETF wrote a co-statement on cryptographic technology and the internet.

RFC:1984

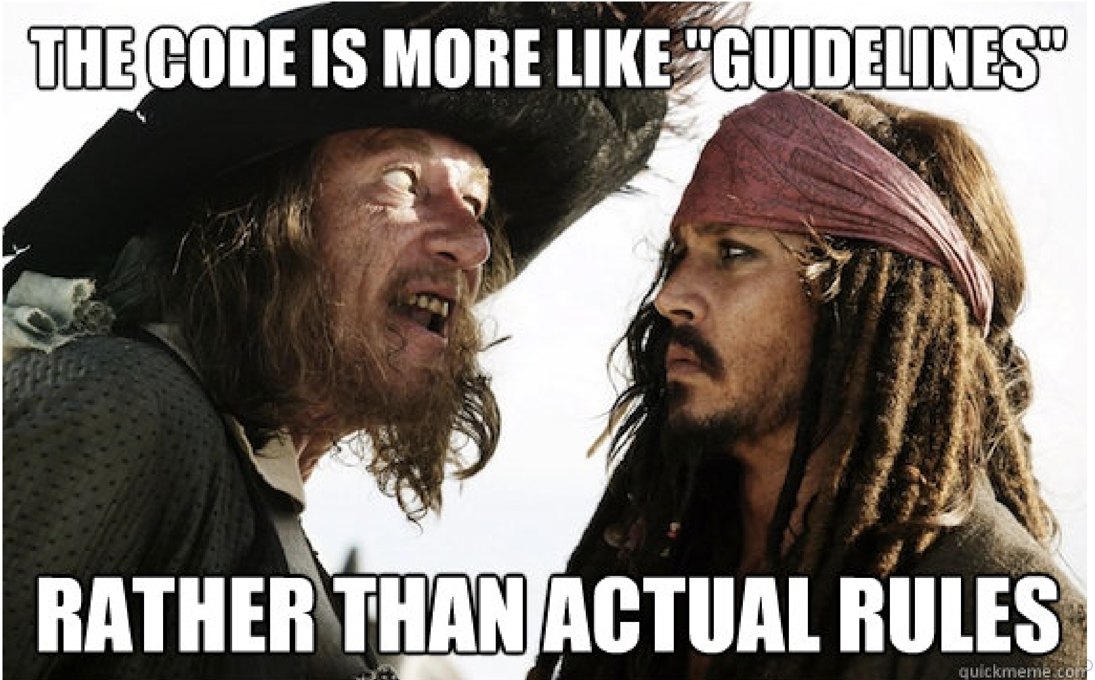
- Brian E. Carpenter of IAB and Fred Baker of IETF wrote a co-statement on cryptographic technology and the internet.
- They felt that there was a need to offer ”All Internet Users an adequate degree of privacy”

RFCs

- What are RFCs?

RFCs

- What are RFCs?
- Can any one submit an RFC?


THE CODE IS MORE LIKE "GUIDELINES"
RATHER THAN ACTUAL RULES
quickmeme.com

RFC:1984

- Brian E. Carpenter of IAB and Fred Baker of IETF wrote a co-statement on cryptographic technology and the internet.
- They felt that there was a need to offer ”All Internet Users an adequate degree of privacy”

RFC:1984

- Brian E. Carpenter of IAB and Fred Baker of IETF wrote a co-statement on cryptographic technology and the internet.
- They felt that there was a need to offer ”All Internet Users an adequate degree of privacy”
- Published in 1996 during US trade embargo on Escrow.

RFC:1984

- Brian E. Carpenter of IAB and Fred Baker of IETF wrote a co-statement on cryptographic technology and the internet.
- They felt that there was a need to offer ”All Internet Users an adequate degree of privacy”
- Published in 1996 during US trade embargo on Escrow.
- Changed to BCP in 2015.

RFC:1984

"The Internet Architecture Board (IAB) and the Internet Engineering Steering Group (IESG),[...] are concerned by the need for increased protection of international commercial transactions on the Internet, and by the need to offer all Internet users an adequate degree of privacy."

RFC:1984

- The IAB and IESG are therefore disturbed to note that various governments have actual or proposed policies on access to cryptographic technology that either:

RFC:1984

- The IAB and IESG are therefore disturbed to note that various governments have actual or proposed policies on access to cryptographic technology that either:
- (a) impose restrictions by implementing export controls; and/or

RFC:1984

- The IAB and IESG are therefore disturbed to note that various governments have actual or proposed policies on access to cryptographic technology that either:
- (a) impose restrictions by implementing export controls; and/or
- (b) restrict commercial and private users to weak and inadequate mechanisms such as short cryptographic keys; and/or

RFC:1984

- The IAB and IESG are therefore disturbed to note that various governments have actual or proposed policies on access to cryptographic technology that either:
- (a) impose restrictions by implementing export controls; and/or
- (b) restrict commercial and private users to weak and inadequate mechanisms such as short cryptographic keys; and/or
- (c) mandate that private decryption keys should be in the hands of the government or of some other third party; and/or

RFC:1984

- The IAB and IESG are therefore disturbed to note that various governments have actual or proposed policies on access to cryptographic technology that either:
- (a) impose restrictions by implementing export controls; and/or
- (b) restrict commercial and private users to weak and inadequate mechanisms such as short cryptographic keys; and/or
- (c) mandate that private decryption keys should be in the hands of the government or of some other third party; and/or
- (d) prohibit the use of cryptology entirely, or permit it only to specially authorized organizations.

What is threatening our privacy?

- Governments looking to put a back door into tools like WhatsApp.

What is threatening our privacy?

- Governments looking to put a back door into tools like WhatsApp.
- Facebook, Google, advertising networks.

What is threatening our privacy?

- Governments looking to put a back door into tools like WhatsApp.
- Facebook, Google, advertising networks.
- Biometric Data including DNA testing services.

What is threatening our privacy?

- Governments looking to put a back door into tools like WhatsApp.
- Facebook, Google, advertising networks.
- Biometric Data including DNA testing services.
- Your family using ALL those services.

Oh come on really?

- Here are a few examples in the UK.

Oh come on really?

- Here are a few examples in the UK.
- David Cameron in 2015 wanted to break encryption: “In our country, do we want to allow a means of communication between people which we cannot read?”

Oh come on really?

- Here are a few examples in the UK.
- David Cameron in 2015 wanted to break encryption: “In our country, do we want to allow a means of communication between people which we cannot read?”
- Draft Investigatory Powers Bill 2015.

Oh come on really?

- Here are a few examples in the UK.
- David Cameron in 2015 wanted to break encryption: “In our country, do we want to allow a means of communication between people which we cannot read?”
- Draft Investigatory Powers Bill 2015.
- In late 2018 GCHQ published ”Principles for a More Informed Exceptional Access Debate.”

What could happen once the data is collected?

- NHS sold some patients data to pharmaceuticals and private healthfirms.

What could happen once the data is collected?

- NHS sold some patients data to pharmaceuticals and private healthfirms.
- EU officials confirmed that UK officials illegally copied data from Shengen Information System.

What could happen once the data is collected?

- NHS sold some patients data to pharmaceuticals and private healthfirms.
- EU officials confirmed that UK officials illegally copied data from Shengen Information System.
- Home office destroyed Windrush data.

What could happen once the data is collected?

- NHS sold some patients data to pharmaceuticals and private healthfirms.
- EU officials confirmed that UK officials illegally copied data from Shengen Information System.
- Home office destroyed Windrush data.
- UK government officials are very careless with data.

America

- July 2019 Attorney General William Barr ”Going Dark” push to require manufacturers of encrypted devices like iPhones to build in a way for law enforcement to gain access, which detractors call ”back doors.”

America

- July 2019 Attorney General William Barr ”Going Dark” push to require manufacturers of encrypted devices like iPhones to build in a way for law enforcement to gain access, which detractors call ”back doors.”
- Palantir being used by ICE to pick up illegal immigrants off the street.

America

- July 2019 Attorney General William Barr ”Going Dark” push to require manufacturers of encrypted devices like iPhones to build in a way for law enforcement to gain access, which detractors call ”back doors.”
- Palantir being used by ICE to pick up illegal immigrants off the street.
- NSA gain access to logs of Americans’ domestic communications under the USA Freedom Act.

America

- July 2019 Attorney General William Barr "Going Dark" push to require manufacturers of encrypted devices like iPhones to build in a way for law enforcement to gain access, which detractors call "back doors."
- Palantir being used by ICE to pick up illegal immigrants off the street.
- NSA gain access to logs of Americans' domestic communications under the USA Freedom Act.
- 2017 Personal Data leak of 198 million US citizens by RNC.

Australia

- Malcolm Turnbull 2015: ”The laws of Australia will trump the laws of mathematics”

Australia

- Malcolm Turnbull 2015: ”The laws of Australia will trump the laws of mathematics”
- Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015

Australia

- Malcolm Turnbull 2015: "The laws of Australia will trump the laws of mathematics"
- Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
- AFP illegally using metadata searches to investigate journalists

Australia

- Malcolm Turnbull 2015: ”The laws of Australia will trump the laws of mathematics”
- Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
- AFP illegally using metadata searches to investigate journalists
- Australia Privacy Amendment act 2017 introduce Notifiable Data Breaches Scheme

Australia: A few example of Breeches

- MyHealth Records 42 Data Breeches in 2018

Australia: A few example of Breeches

- MyHealth Records 42 Data Breeches in 2018
- German Researchers found sensitive medical data on unsecured servers worldwide.

Australia: A few example of Breeches

- MyHealth Records 42 Data Breeches in 2018
- German Researchers found sensitive medical data on unsecured servers worldwide.
- Queensland Health lost records in July 2019

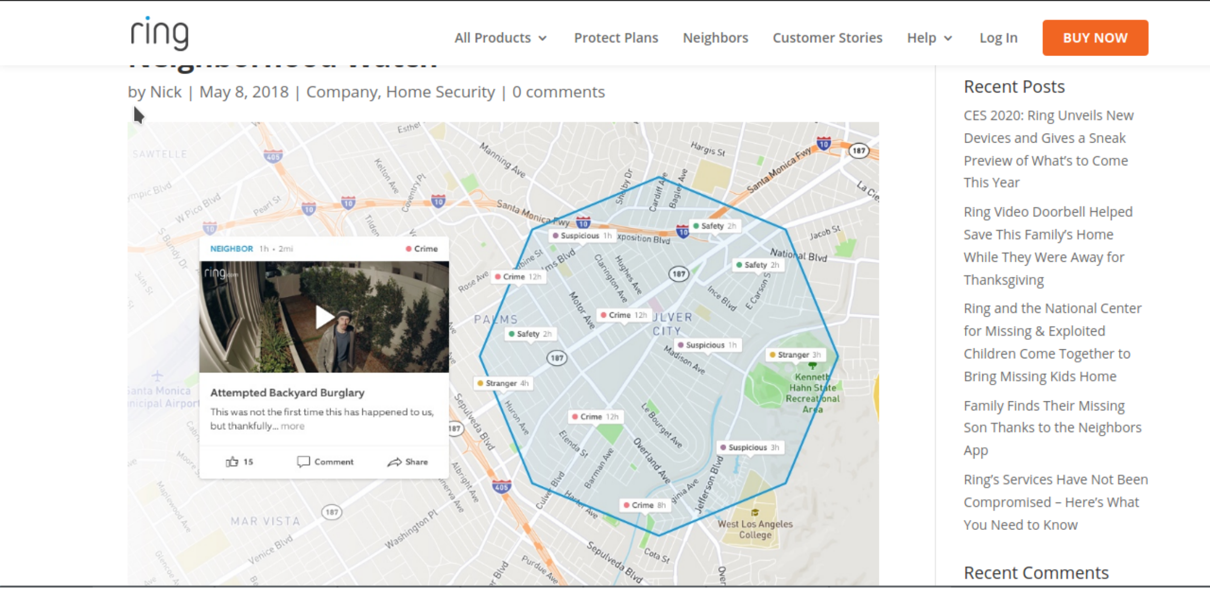
Australia: A few example of Breeches

- MyHealth Records 42 Data Breeches in 2018
- German Researchers found sensitive medical data on unsecured servers worldwide.
- Queensland Health lost records in July 2019
- ANU Data Breech 19 years of Academic Records

Australia: A few example of Breeches

- MyHealth Records 42 Data Breeches in 2018
- German Researchers found sensitive medical data on unsecured servers worldwide.
- Queensland Health lost records in July 2019
- ANU Data Breech 19 years of Academic Records
- Public Transport Victoria (PTV) location data Myki breech.

ring



by Nick | May 8, 2018 | Company, Home Security | 0 comments

Attempted Backyard Burglary

This was not the first time this has happened to us, but thankfully... more

Recent Posts

CES 2020: Ring Unveils New Devices and Gives a Sneak Preview of What's to Come This Year

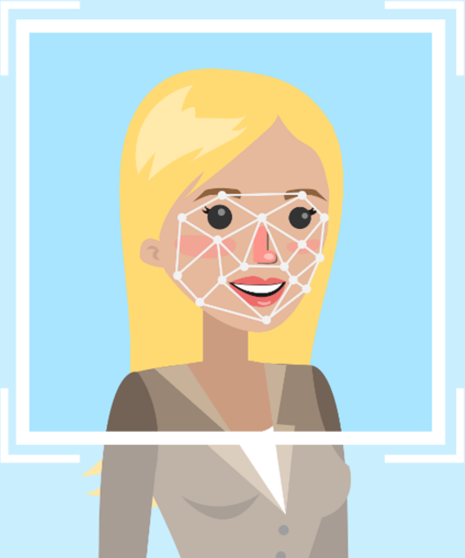
Ring Video Doorbell Helped Save This Family's Home While They Were Away for Thanksgiving

Ring and the National Center for Missing & Exploited Children Come Together to Bring Missing Kids Home

Family Finds Their Missing Son Thanks to the Neighbors App

Ring's Services Have Not Been Compromised – Here's What You Need to Know

Recent Comments



Facial Recognition

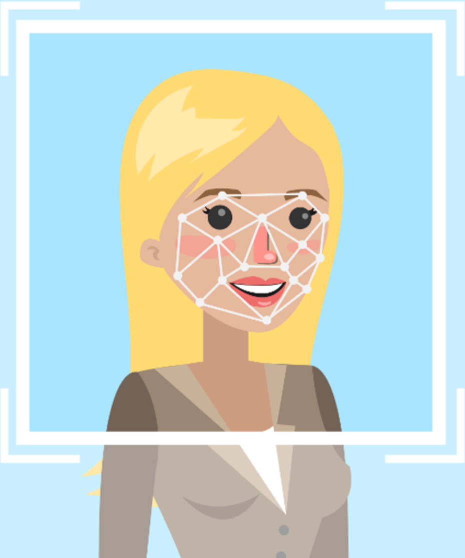
- Government

Facial Recognition

- Government
- Schools

Facial Recognition

- Government
- Schools
- Consumer Products



But Ancestry DNA testing isn't really a threat

- Buzzfeed Investigation

But Ancestry DNA testing isn't really a threat

- Buzzfeed Investigation
- GEDMatch

But Ancestry DNA testing isn't really a threat

- Buzzfeed Investigation
- GEDMatch
- Commercial DNA testing

But Ancestry DNA testing isn’t really a threat

- Buzzfeed Investigation
- GEDMatch
- Commercial DNA testing
- Conclusion: On it’s own no. But as part of a possible dataset combined with other metadata?

So do we need Privacy?

- It's too late my family are all on it.

So do we need Privacy?

- It's too late my family are all on it. Yes, and they are still a risk to your privacy.

So do we need Privacy?

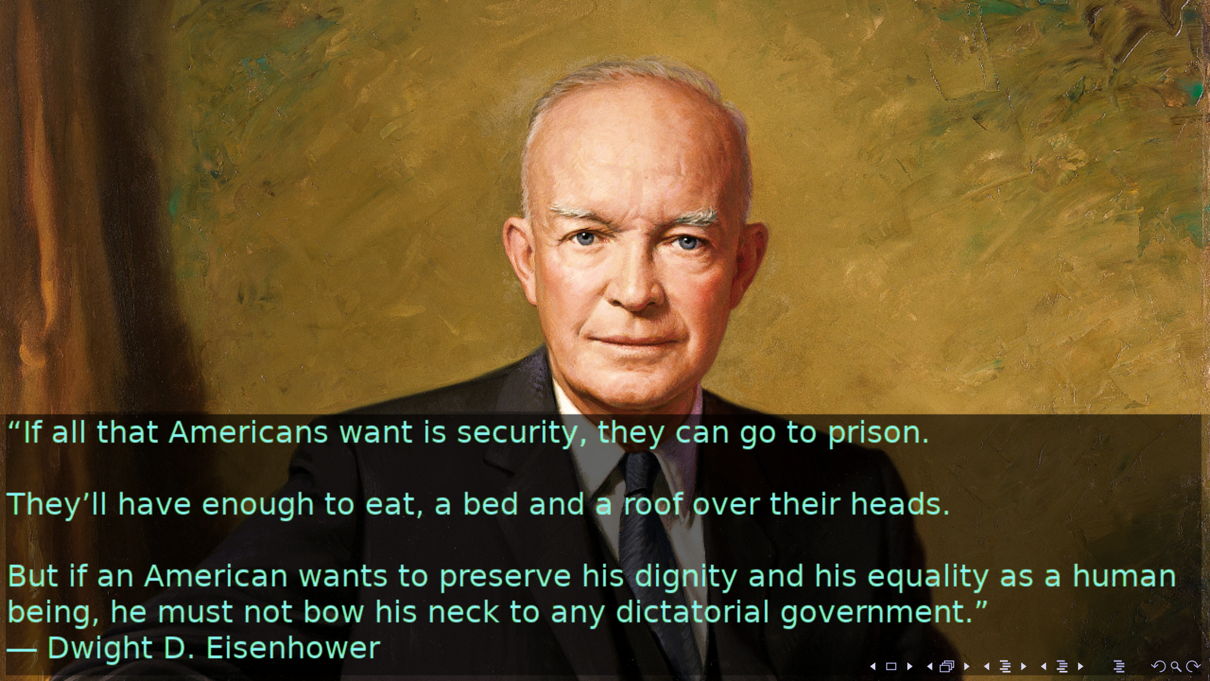
- It's too late my family are all on it. Yes, and they are still a risk to your privacy.
- Even teenagers don't care.

So do we need Privacy?

- It's too late my family are all on it. Yes, and they are still a risk to your privacy.
- Even teenagers don't care. Not true, teenagers are private.

So do we need Privacy?

- It's too late my family are all on it. Yes, and they are still a risk to your privacy.
- Even teenagers don't care. Not true, teenagers are private.
- We need to give up a little privacy for our security.



“If all that Americans want is security, they can go to prison.

They’ll have enough to eat, a bed and a roof over their heads.

But if an American wants to preserve his dignity and his equality as a human being, he must not bow his neck to any dictatorial government.”
— Dwight D. Eisenhower

So do we need Privacy?

- It's too late my family are all on it. Yes, and they are still a risk to your privacy.
- Even teenagers don't care. Not true, teenagers are private.
- We need to give up a little privacy for our security. What defines our Security?

Is there hope ?

- Mainstream Press starting to publish the dangers

Is there hope ?

- Mainstream Press starting to publish the dangers
- Certain Cities in the US banning facial recognition

Is there hope ?

- Mainstream Press starting to publish the dangers
- Certain Cities in the US banning facial recognition
- Conferences like Linux.Conf.Au

What can we do?

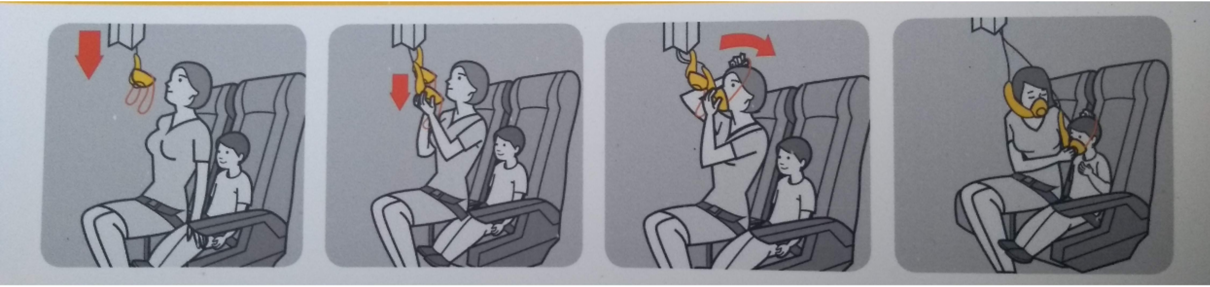
- Do your own research.

What can we do?

- Do your own research.
- Build in privacy.

What can we do?

- Do your own research.
- Build in privacy.
- Follow privacy focused organisations online.



What can we do?

- Do your own research.
- Build in privacy.
- Follow privacy focused organisations and people online.
- Protect your own privacy.

What can we do?

- Do your own research.
- Build in privacy.
- Follow privacy focused organisations and people online.
- Protect your own privacy.
- Join decentralised networks like Mastodon and Diaspora.

What can we do?

Use stories to help people to empathise and understand.

What can we do?

- Use stories to help people to empathise and understand.
- Focus on Io, not Argus Panoptes.

Final thoughts

- Find ways to frame the dialogue around privacy

Final thoughts

- Find ways to frame the dialogue around privacy
- Use your own culture's stories where possible to help people empathise about the dangers

Final thoughts

- Find ways to frame the dialogue around privacy
- Use your own culture's stories where possible to help people empathise about the dangers
- Contact your political representatives

Final thoughts

- Find ways to frame the dialogue around privacy
- Use your own culture's stories where possible to help people empathise about the dangers
- Contact your political representatives
- Encourage friends and family to contact their representatives

Final thoughts

- Human rights violations are here now.

Final thoughts

- Human rights violations are here now.
- It’s important to not normalise the virtual panopticon

Use the hashtag #RFC1984

Questions?

e-mail: esther@gladserv.com
https://www.linkedin.com/in/estherpayne/
twitter: @onepict
mastodon: @onepict@fosstodon.org
telegram: @onepict