



# RFC 1984:

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

presentation by: Esther Payne at Ubucon Europe 2019



Ubucon Europe  
Sintra | Portugal

## About me

IT Professional with 20 years in Support.  
Over a decade working in Opensource at  
Gladserv.

**e-mail:** [esther@gladserv.com](mailto:esther@gladserv.com)

**LinkedIn:** <https://www.linkedin.com/in/estherpayne/>

**twitter:** @onepict

**telegram:** @onepict



# Do we need Privacy?



# 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





# Storytime

- ▶ Humans learn from stories

# Storytime

- ▶ Humans learn from stories
- ▶ Fables by Aesop

# Storytime

- ▶ Humans learn from stories
- ▶ Fables by Aesop
- ▶ and on to Greek mythology....



# Ovid and greek myths

- ▶ Who was Ovid?

# Ovid and greek myths

- ▶ Who was Ovid?
- ▶ What did he write?

# Ovid and greek myths

- ▶ Who was Ovid?
- ▶ What did he write?
- ▶ why....



# What does this have to do with Peacocks?

- ▶ Well I love a peacock feather.....

# What does this have to do with Peacocks?

- ▶ Well I love a peacock feather.....
- ▶ So did Ovid.. which leads us on to...

# Io and Argus

- ▶ Io and Argus

# Io and Argus

- ▶ Io and Argus
- ▶ Ovid updated the story

# Io and Argus

- ▶ Io and Argus
- ▶ Ovid updated the story
- ▶ BY ADDING PEACOCKS!



# 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.

# 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.
- ▶ Not ideal as a symbol!

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.

# 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"

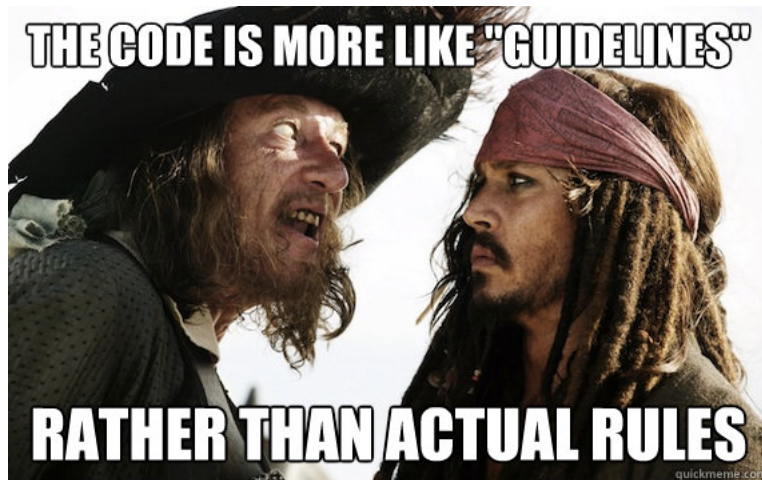
# RFCs

- ▶ What are RFCs?

# RFCs

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

Does anyone use RFCs



## 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.
- ▶ Not a new issue. Infact it's been a concern since the 1960s. Before the internet.

"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.
- ▶ DNA testing services.



# What is threatening our privacy?

- ▶ Governments looking to put a back door into tools like WhatsApp.
- ▶ Facebook, Google, advertising networks.
- ▶ 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 of 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 of 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 of the street
- ▶ NSA gain access to logs of Americans' domestic communications under the USA Freedom Act.
- ▶ NSA program permits the mapping of relationships of targeted individuals/comunities

# 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 of the street
- ▶ NSA gain access to logs of Americans' domestic communications under the USA Freedom Act.
- ▶ NSA program permits the mapping of relationships of targeted individuals/comunities
- ▶ 2017 Electoral Data of 200 million US citizens

# 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
- ▶ AFC illegally using metadata to track journalists

# Australia

- ▶ Malcolm Turnbull 2015: "The laws of Australia will trump the laws of mathematics"
- ▶ Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
- ▶ AFC illegally using metadata to track journalists
- ▶ German Researchers found sensitive medical data on unsecured servers worldwide.

# Australia

- ▶ Malcolm Turnbull 2015: "The laws of Australia will trump the laws of mathematics"
- ▶ Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
- ▶ AFC illegally using metadata to track journalists
- ▶ German Researchers found sensitive medical data on unsecured servers worldwide.
- ▶ Public Transport Victoria (PTV) data leak of tap on tap off cards



# 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?

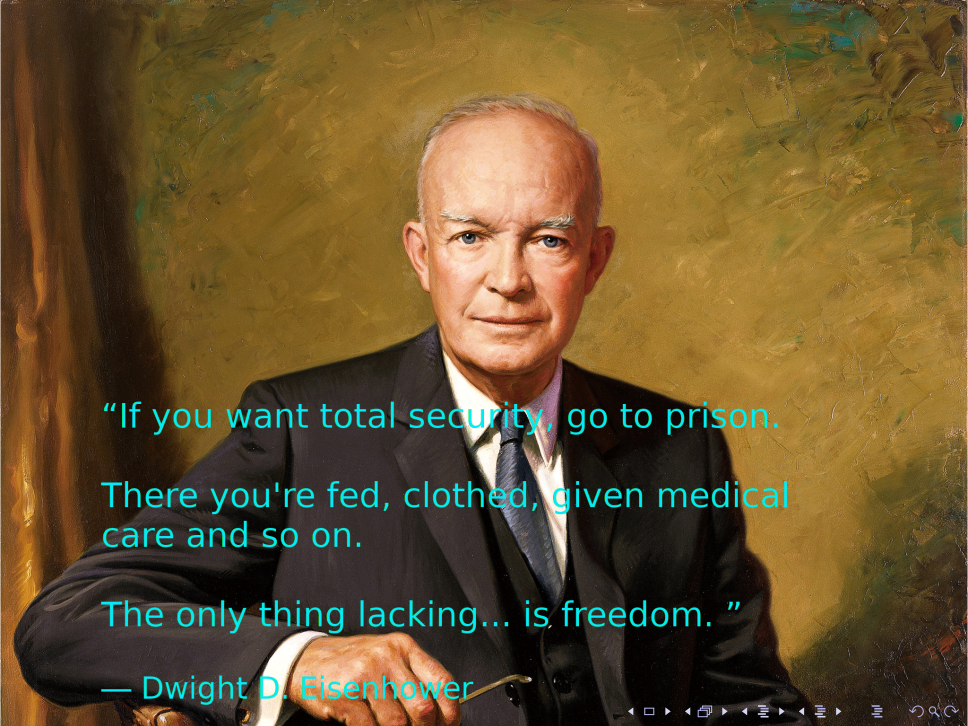
- ▶ It's too late my family are all on it. Yes, and they are still a risk to your privacy.
- ▶ Even teenagers don't care.

## 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.

A portrait of Dwight D. Eisenhower, an elderly man with white hair, wearing a dark suit, white shirt, and blue tie. He is holding a pair of glasses in his right hand. The background is a textured, olive-green and brownish-yellow color.

“If you want total security, go to prison.

There you're fed, clothed, given medical care and so on.

The only thing lacking... is freedom. ”

— 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.

# 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?



# 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?
- ▶ Privacy isn't dead. Infact I'd argue it's a feature of Civilisation.

# What can we do?

- ▶ Do your own research.

# What can we do?

- ▶ Do your own research.
- ▶ Follow IETF and IAB.

# What can we do?

- ▶ Do your own research.
- ▶ Follow IETF and IAB.
- ▶ Follow privacy focused organisations and people online.



# What can we do?

- ▶ Do your own research.
- ▶ Follow IETF and IAB.
- ▶ Follow privacy focused organisations and people online.
- ▶ Protect your own privacy

# What can we do?

- ▶ Do your own research.
- ▶ Follow IETF and IAB.
- ▶ Follow privacy focused organisations and people online.
- ▶ Protect your own privacy
- ▶ Join Decentralised networks like mastodon.

# What can we do?

- ▶ Do your own research.
- ▶ Follow IETF and IAB.
- ▶ Follow privacy focused organisations and people online.
- ▶ Protect your own privacy
- ▶ Join Decentralised networks like mastodon.
- ▶ Look at projects like Framasoft and their CHATONS partners campaign to "degooglify the internet".



# What can we do?

- ▶ Start talking to your family and friends

# What can we do?

- ▶ Start talking to your family and friends
- ▶ Use stories to help them empathise and understand. Focus on Io, not Argus Panoptes



- ▶ Use your own cultures stories where possible to help people empathise about the dangers

- ▶ Use your own cultures stories where possible to help people empathise about the dangers
- ▶ Use the hashtag #RFC1984

- ▶ Use your own cultures stories where possible to help people empathise about the dangers
- ▶ Use the hashtag #RFC1984
- ▶ Read 1984 and think about the surveillance and what it means.

- ▶ Use your own cultures stories where possible to help people empathise about the dangers
- ▶ Use the hashtag #RFC1984
- ▶ Read 1984 and think about the surveillance and what it means.

# Final thoughts

- ▶ Find ways for us to frame the dialogue around privacy



# Final thoughts

- ▶ Find ways for us to frame the dialogue around privacy
- ▶ Human rights violations are here now.

# Final thoughts

- ▶ Find ways for us to frame the dialogue around privacy
- ▶ Human rights violations are here now.
- ▶ Perhaps we can keep using Peacocks as a symbol



# Final thoughts

- ▶ Grass root campaigns are vital to start putting pressure on governments and organisations

# Final thoughts

- ▶ Grass root campaigns are vital to start putting pressure on governments and organisations
- ▶ Start now.



# RFC 1984:

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

presentation by: Esther Payne at Ubucon Europe 2019

Thank you

