

RFC 1984:

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

Esther Payne

FOSSASIA SUMMIT SINGAPORE 21st March 2020



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.



Humans learn from stories



Io and Argus





Branding Argus Panoptes





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"

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.

"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."

- ▶ 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.

Political Threats

- ▶ Here are a few examples from 3 of the 5 eyes.

Political Threats

- ▶ Here are a few examples from 3 of the 5 eyes.
- ▶ David Cameron and Malcolm Turnbull in 2015 wanted to break encryption

Political Threats

- ▶ Here are a few examples from 3 of the 5 eyes.
- ▶ David Cameron and Malcolm Turnbull in 2015 wanted to break encryption
- ▶ Draft Investigatory Powers Bill 2015 in UK and Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 in Australia.

Political Threats

- ▶ Here are a few examples from 3 of the 5 eyes.
- ▶ David Cameron and Malcolm Turnbull in 2015 wanted to break encryption
- ▶ Draft Investigatory Powers Bill 2015 in UK and Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 in Australia.
- ▶ July 2019 and in January 2020 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."

Political Threats

- ▶ Here are a few examples from 3 of the 5 eyes.
- ▶ David Cameron and Malcolm Turnbull in 2015 wanted to break encryption
- ▶ Draft Investigatory Powers Bill 2015 in UK and Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 in Australia.
- ▶ July 2019 and in January 2020 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."
- ▶ NSA gain access to logs of Americans' domestic communications under the USA Freedom Act.

Political Threats

- ▶ Here are a few examples from 3 of the 5 eyes.
- ▶ David Cameron and Malcolm Turnbull in 2015 wanted to break encryption
- ▶ Draft Investigatory Powers Bill 2015 in UK and Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 in Australia.
- ▶ July 2019 and in January 2020 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."
- ▶ NSA gain access to logs of Americans' domestic communications under the USA Freedom Act.
- ▶ Various Legislation proposals like Earn IT act (US), Online Harms (UK)

Political Threats

- ▶ Here are a few examples from 3 of the 5 eyes.
- ▶ David Cameron and Malcolm Turnbull in 2015 wanted to break encryption
- ▶ Draft Investigatory Powers Bill 2015 in UK and Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 in Australia.
- ▶ July 2019 and in January 2020 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."
- ▶ NSA gain access to logs of Americans' domestic communications under the USA Freedom Act.
- ▶ Various Legislation proposals like Earn IT act (US), Online Harms (UK)
- ▶ Political parties collecting Data on Constituents

Political Threats

- ▶ Here are a few examples from 3 of the 5 eyes.
- ▶ David Cameron and Malcolm Turnbull in 2015 wanted to break encryption
- ▶ Draft Investigatory Powers Bill 2015 in UK and Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015 in Australia.
- ▶ July 2019 and in January 2020 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."
- ▶ NSA gain access to logs of Americans' domestic communications under the USA Freedom Act.
- ▶ Various Legislation proposals like Earn IT act (US), Online Harms (UK)
- ▶ Political parties collecting Data on Constituents
- ▶ Various emergency powers granted to Governments to combat COVID-19

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.
- ▶ German Researchers found sensitive medical data on unsecured servers worldwide.

What could happen once the data is collected?

- ▶ NHS sold some patients data to pharmaceuticals and private healthfirms.
- ▶ German Researchers found sensitive medical data on unsecured servers worldwide.
- ▶ EU officials confirmed that UK officials illegally copied data from Schengen Information System.

What could happen once the data is collected?

- ▶ NHS sold some patients data to pharmaceuticals and private healthfirms.
- ▶ German Researchers found sensitive medical data on unsecured servers worldwide.
- ▶ EU officials confirmed that UK officials illegally copied data from Schengen Information System.
- ▶ 2017 Personal Data leak of 198 million US citizens by RNC.

What could happen once the data is collected?

- ▶ NHS sold some patients data to pharmaceuticals and private healthfirms.
- ▶ German Researchers found sensitive medical data on unsecured servers worldwide.
- ▶ EU officials confirmed that UK officials illegally copied data from Schengen Information System.
- ▶ 2017 Personal Data leak of 198 million US citizens by RNC.
- ▶ Home office destroyed Windrush data.

What could happen once the data is collected?

- ▶ NHS sold some patients data to pharmaceuticals and private healthfirms.
- ▶ German Researchers found sensitive medical data on unsecured servers worldwide.
- ▶ EU officials confirmed that UK officials illegally copied data from Schengen Information System.
- ▶ 2017 Personal Data leak of 198 million US citizens by RNC.
- ▶ Home office destroyed Windrush data.
- ▶ Palantir being used by ICE to pick up illegal immigrants off the street.

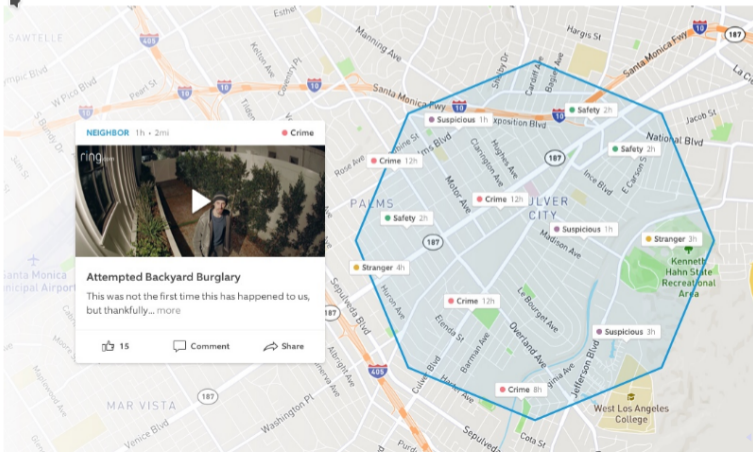
What could happen once the data is collected?

- ▶ NHS sold some patients data to pharmaceuticals and private healthfirms.
- ▶ German Researchers found sensitive medical data on unsecured servers worldwide.
- ▶ EU officials confirmed that UK officials illegally copied data from Schengen Information System.
- ▶ 2017 Personal Data leak of 198 million US citizens by RNC.
- ▶ Home office destroyed Windrush data.
- ▶ Palantir being used by ICE to pick up illegal immigrants off the street.
- ▶ UK government officials are very careless with data.





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



Recent Posts

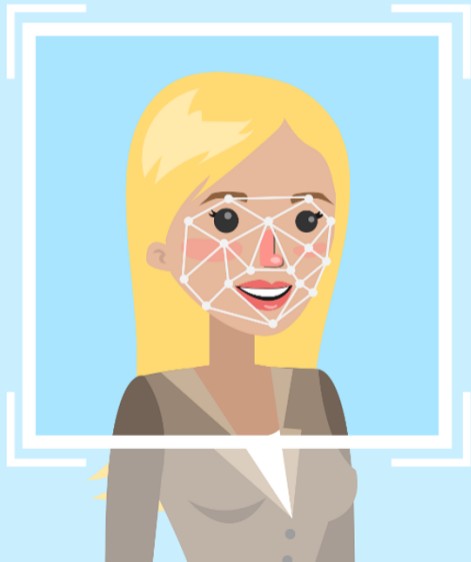
[CES 2020: Ring Unveils New Devices and Gives a Sneak Preview of What's to Come This Year](#)

[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](#)



Facial Recognition

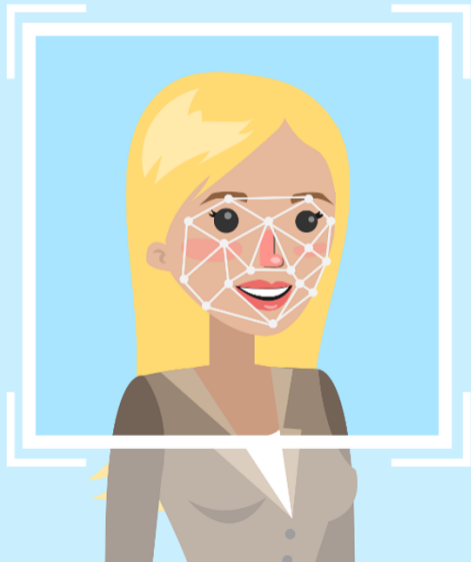
- ▶ Government

Facial Recognition

- ▶ Government
- ▶ Schools

Facial Recognition

- ▶ Government
- ▶ Schools
- ▶ Consumer Products



DNA and Medical

- ▶ DNA testing kits and law enforcement

DNA and Medical

- ▶ DNA testing kits and law enforcement
- ▶ Medicare and PBS history of over 2.5 million Australians being re-identifiable online

DNA and Medical

- ▶ DNA testing kits and law enforcement
- ▶ Medicare and PBS history of over 2.5 million Australians being re-identifiable online
- ▶ Systems developing biometric identification including gait etc.

DNA and Medical

- ▶ DNA testing kits and law enforcement
- ▶ Medicare and PBS history of over 2.5 million Australians being re-identifiable online
- ▶ Systems developing biometric identification including gait etc.
- ▶ 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.

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. Are we prepared to sacrifice our freedom and dignity?



Is there hope?

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
- ▶ YOU!

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.

What I spoke about in my day job at Ubucon Europe.

<https://sintra2019.ubucon.org/>

<https://youtu.be/ZVXT0jz4dZI>

Ubucon Europe 2019 - RFC 1984 Or why you should start worrying about encryption backdoors and mass data collection.

I even talk about mythology and Peacocks. It's about 40 minutes long.



SINTRA2019.UBUCON.ORG

Ubucon Europe 2019 – Sintra, 10th-13th October

Ubucon is an event organized by the Ubuntu Communities from all around...

Brett Sheffield, and 2 others

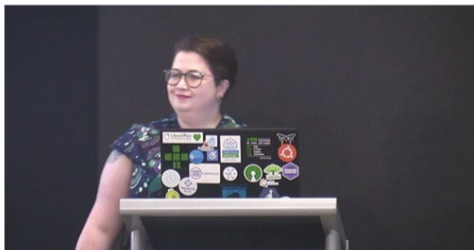


Your post

I did a talk at a conference in Australia about Ovid, Greek Mythology and also privacy online. So I think there might be something for everybody. Plus there are peacocks.

This isn't a talk where I rant about people using facebook. Facebook is a very useful tool for families, friends and community.

But Privacy is a complex thing, how do we make ourselves a bit more aware of what the technology does and what risks does it hold? Should we be holding our governments to account more?



YOUTUBE.COM

RFC 1984: Or why you should start worrying about encryption backdoors and mass data collection

Brett Sheffield,

and 24 others

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@librecast.net

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

twitter: @onepict

mastodon: @onepict@chaos.social

telegram: @onepict

THE CODE IS MORE LIKE "GUIDELINES"



RATHER THAN ACTUAL RULES