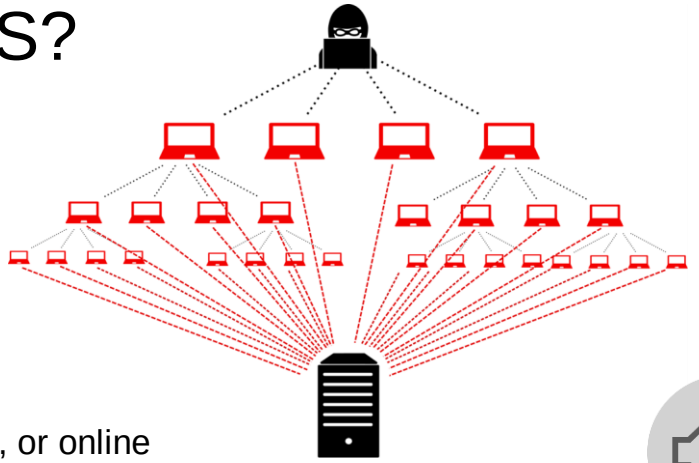
Laws of Computer Crime

US vs UK

DDoS

What is DDoS?



- A distributed denial-of-service attacks goal, is to render a website, or online service inoperable, by overwhelming them, flooding the host with too much traffic requests. It also can have a financial hit on the target.

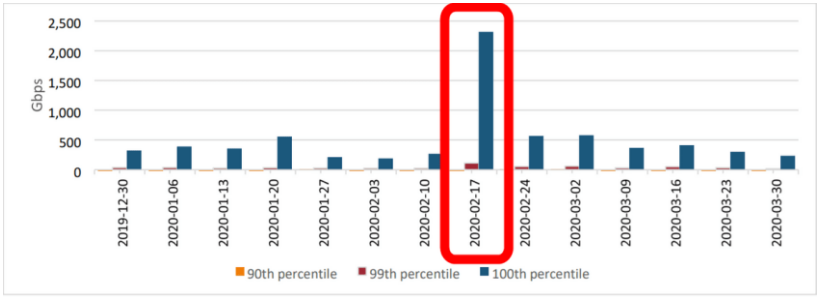


Figure 2. P90, P99, and P100 of volumetric events, measured in gigabits per second (Gbps), for resources on AWS during Q1 2020.

[AWS 2.3 Tbps attack in 2020]

The increase over the years

- DDoS attacks have increased by 151 percent in first half of 2020.
- As more and more devices become available for a cheaper price(IoT etc.), We can expect a substantial growth of attacks every year.

But is it possible to do anything about it? Should We bear these attacks without any regulations? Well, fortunately, they are illegal. But how illegal?

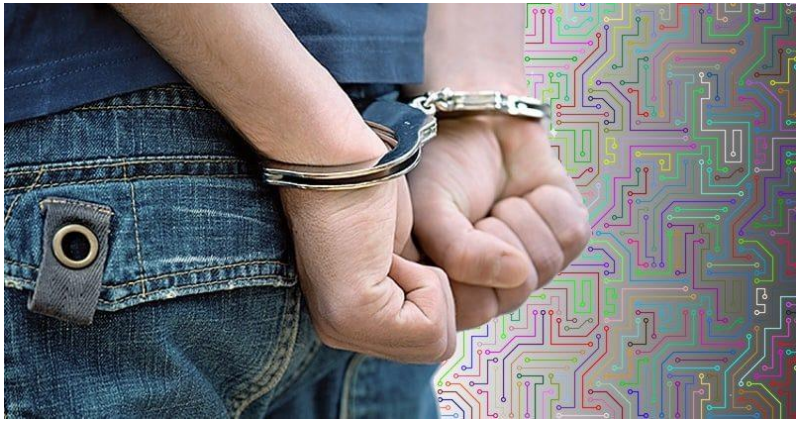
Computer Misuse Act (‘CMA’)

- The Computer Misuse Act 1990 makes it illegal to intentionally impair the operation of a computer or prevent or hinder access to a program/data on a computer unless you are authorised to do so.

What this means, is that DDoS attacks fall under the UK laws, and can be punishable by a prison sentence up to 10 years, plus fines.

From this, We can clearly see, that these type of attacks stress organisations, businesses, and individuals.

- Section 3



- **A British teenager has been sentenced for his part in what was called the "biggest cyber attack in history".**
  Spamhaus attack 2013

Computer Fraud and Abuse Act (‘CFAA’)

- The federal CFAA is the primary statutory mechanism for prosecuting cybercrime, and it provides both criminal and civil penalties.

- It states, that it prohibits either knowingly intentionally or recklessly damaging a computer.

- “Whoever knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;” CFAA (a)(5)(A)

- DDoS attacks may be subject to civil and criminal liability, including fine and imprisonment (for up to 10 years), under state and federal law.

US cases

- In 2013 the grand jury in Virginia indicted 13 Anonymous members for knowingly taking part in Denial-of-Service attacks. Where, the question came up of whether DDoS-ing a website violates the CFAA or not, because of an another case: Pulte Homes, Inc. v. Laborers' Int'l Union.

- What if We push the refresh button without stopping? What if We ask our friends to help in our clicking contest? What if a python script would do the same? What can do this? Should DDoS be used as a form of protest?

- Does this fit into a 21st century cybersecurity law? Is this appropriate?

LiUNA!

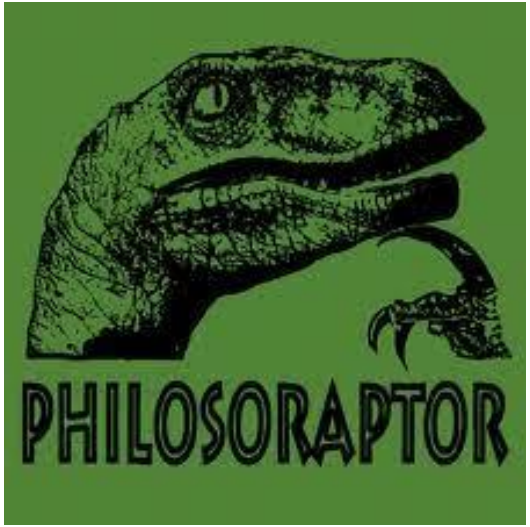
Feel the Power

vs

Pulte HOMES

Summary

- Is it better to do it in the UK or the US?
- A form of damaging property, causing problems hidden behind the act of protesting?
- 10 years of imprisonment, and/or additional fines to pay? Is it too much or not enough?
- Is me mistakenly requesting, clicking a weaker webservice a thousand times a second with a broken mouse denial-of-service?



Copyright infringement

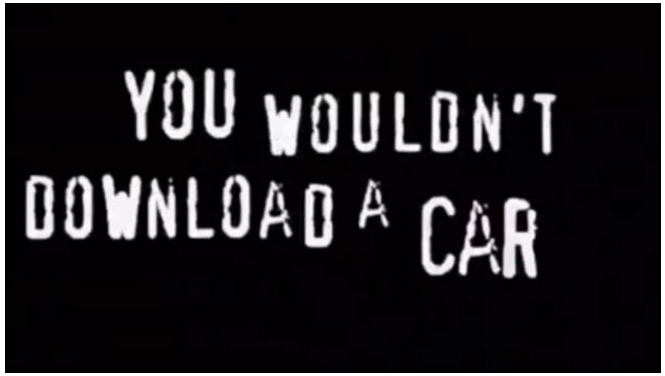
US vs UK

What counts as ‘copyright infringement’?

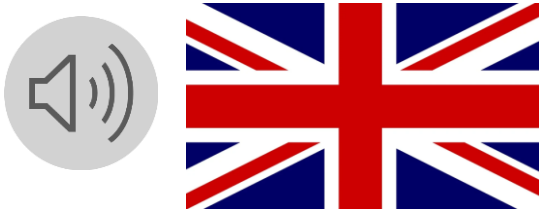
“IP rights are infringed when a product, creation or invention protected by IP laws are exploited, copied or otherwise used without having the proper authorisation.” *(Intellectual Property Office, 2016)*

IP covers copyright, trademarks, patents etc.

Generally, this means that a given copyright holder has the exclusive right to reproduce, prepare derivative works, produce copies or give copies to others and perform or display that given work - and by doing this without the permission of the copyright owner - you’re infringing their copyright.
(Wikisource, 2020)(UK Government, No date A)



UK laws



Copyright Designs and patents act 1988 - General copyright law, covers:

> “original literary, dramatic, musical or artistic works, sound recordings, films or broadcasts and the typographical arrangement of published editions.” *(UK Government Legislation, No date A)*

The copyright (computer programs) regulations 1992:

> Extended the definition of a computer program to be covered under the ‘Literary works’ aspect of the CDPA. *(UK Government Legislation, No date B)*

Digital Economy act 2017:

> Amended copyright designs and patents act to increase possible sentence for internet copyright infringement from 2 years to 10 years. *(UK Government Legislation, No date C)*

US Laws

Copyright act of 1976 - General copyright law covers:

“literary works, musical works, including any accompanying words, dramatic works, including any accompanying music, pantomimes and choreographic works, pictorial, graphic, and sculptural works, motion pictures and other audiovisual works, and sound recordings.” *(IT Law Wikia, no date)*

As per this - computer programs covered under ‘literary works’.

No electronic theft act (1997) - prior to this you could only be prosecuted if your copyright infringement was for “Commercial advantage or financial gain.” - changed to “receipt, or expectation of receipt of anything of value.” but this still didn’t apply to sites who don’t receive anything, so they also added a stipulation that if you were to during any 180 day period distribute any copyrighted works which have a total retail value of $1000 - then you were breaking the law. *(Congress, no date)*

The Digital Millennium Copyright Act(1998) - This act was largely used to stop copyright infringement by using online service providers - it allows a copyright holder to send a DMCA claim if they believe their copyright is being infringed on the internet - if you receive a DMCA claim your OSP must remove the content the claim was on if it meets the requirement of a DMCA claim - as they have no right to judgement of the content *(Digital Media Law Project, No date A)*, it’s not their job to decide if it is copyright infringing and by doing so would open themselves up legal action themselves - they lose “Safe Harbour” status *(Digital Media Law Project, No date B)(Electronic Frontier Foundation, No date)*. The onus is on the user who uploaded the content to file a counter claim to have it brought back, not the OSP.

UK compared to the US

Punishment - UK has a max punishment of 10 years and an ‘unlimited’ fine *(Crown Prosecution Service, 2019)* - US has a max criminal punishment of five years or a max fine of $250,000 *(Recording Industry Association of America, No Date)*. Civil penalties can include damages of up to $150,000 *(Cornell law school, No date)*. Individuals have been prosecuted for up to $220,000.*(Holpuch, 2012)*

No DMCA equivalent - In the UK a Copyright holder can’t legally file a takedown notice against a website easily, but a host must take down copyrighted content if they’re aware of it - and if they don’t after being made aware they *can* have an injunction issued against them *(Bird&Bird, 2015)*.

Generally speaking both do nothing nowadays - In both the US and UK - BPI and RIAA, who were the main groups involved in prosecuting copyright infringement stopped suing individuals more than 10 years ago and moved onto acting with ISP’s *(Silverman, 2008)*.

Prevention from prosecution - Both prevent ISP’s from being prosecuted so long as they are unaware of the copyright infringement, but become liable if they don’t remove content once they’re made aware of it.

Are these legislations fit for purpose?

Not really, no. If a copyright owner wishes to take action against an individual who is infringing on their copyright - they have the means to do so under both countries existing legislation, but prosecuting people under this has not stopped digital copyright infringement in any significant way.

For example in the mid 2000's the RIAA attempted to sue at least 18,000 people for some type of file sharing *(Anderson, 2009)*. Most were settled outside of court for tiny amounts or just not prosecuted, in a 3 year period between 2006-2008 they spent $64 million to get roughly $1.4 million back *(Recording Industry vs The people, 2010)* - as well as other disastrous cases including one where they sued a dead person *(Orlowski, 2005)* - so taking action against individuals proved to be almost completely pointless.

Generally speaking companies and groups have moved from direct legal action to cooperating with ISP's through agreements to take down infringing websites *(British Phonographic Industry, 2020)*, though these are not laws nor are they legally binding. The UK has a unique code in collaboration with Bing and Google *(UK Government, 2017)*, and claims to have reduced piracy by 26% overall through their 'Get it right' campaigning *(ISPreview, 2019)*.

Ironically, one of the more efficient pieces of legislation between the two nations (DMCA) is also arguably one of the worst - due to the DMCA allowing for very quick removal of allegedly 'copyrighted content' with the user being responsible for filing a counterclaim and dealing with the complicated nature of copyright law, meaning a lot won't bother or have to go through expensive court procedures. According to a 2009 article, google stated that 57% of it's DMCA takedowns were businesses targeting competitors *(European Digital Rights, 2012)*, which illustrates how rife with abuse it can be.

References (in order of use)

Intellectual Property Office (2016) *Intellectual Property Crime and Infringement.* https://www.gov.uk/guidance/intellectual-property-crime-and-infringement Accessed 04/02/21

Wikisource (2020) *Copyright act of 1976* https://en.wikisource.org/wiki/Copyright_Act_of_1976#%C2%A7_106._Exclusive_rights_in_copyrighted_works Accessed 04/02/21

UK Government (No date) *How copyright protects your work*. https://www.gov.uk/copyright Accessed 04/02/21

UK Government Legislation (No date A) *Copyright, Designs and Patents act 1988* https://www.legislation.gov.uk/ukpga/1988/48/section/1#commentary-c19313581 Accessed 04/02/21

UK Government Legislation (No date B) *The Copyright (Computer Programs) Regulations 1992* https://www.legislation.gov.uk/uksi/1992/3233/crossheading/amendments-of-part-i-copyright-of-the-copyright-designs-and-patents-act-1988/made Accessed 04/02/21

UK Government Legislation (No date C) *Digital Economy Act 2017* https://www.legislation.gov.uk/ukpga/2017/30/section/32/enacted Accessed 04/02/21

IT Law Wikia (No date) *1976 Copyright Act*. https://itlaw.wikia.org/wiki/1976_Copyright_Act Accessed 04/02/21

Congress (No date) *No Electronic Theft (NET) Act* https://www.congress.gov/105/plaws/publ147/PLAW-105publ147.pdf Accessed 04/02/21

Digital Media Law Project (No date A) *Responding to a DMCA Takedown Notice Targeting Your Content* https://www.dmlp.org/legal-guide/responding-dmca-takedown-notice-targeting-your-content accessed 05/02/21

Digital Media Law Project (No date B) *Protecting Yourself Against Copyright Claims Based on User Content.* https://www.dmlp.org/legal-guide/protecting-yourself-against-copyright-claims-based-user-content accessed 05/02/21

Electronic Frontier Foundation (No date) *DMCA* https://www.eff.org/issues/dmca accessed 05/02/21

Crown Prosecution Service (2019) *Intellectual Property Crime* https://www.cps.gov.uk/legal-guidance/intellectual-property-crime accessed 05/02/21

Recording Industry Association of America (No date) *About Piracy* https://www.riaa.com/resources-learning/about-piracy/ accessed 05/02/21

Cornell Law School (No date) *Remedies for Infringement: Damages and profits* https://www.law.cornell.edu/uscode/text/17/504 accessed 05/02/21

Holpuch, A (2012) *'Minnesota woman to pay $220,000 fine for 24 illegally downloaded songs'*, The Guardian, 11 September, https://www.theguardian.com/technology/2012/sep/11/minnesota-woman-songs-illegally-downloaded accessed 05/02/21

Bird&Bird (2015) *IP & IT Bytes: website blocking order against internet service providers* https://www.twobirds.com/en/news/articles/2015/global/ip-and-it-law-bytes-june/copyright-website-blocking-order-against-internet-service-providers Accessed 05/02/21

Silverman, D (2008) *Why the Recording Industry Really Stopped Suing Its Customers*, Harvard Business Review, 22 December, https://hbr.org/2008/12/why-the-riaa-stopped-suing Accessed 05/02/21

Anderson, N (2009) *Has the RIAA sued 18,000 people… or 35,000?* ArsTechnica, 8 July, https://arstechnica.com/tech-policy/2009/07/has-the-riaa-sued-18000-people-or-35000/ Accessed 05/02/21

Recording Industry vs The People (2010) *ha ha ha ha ha. RIAA paid it's lawyers more than $16,000,000 in 2008 to recover only $391,000!!!* http://recordingindustryvspeople.blogspot.com/2010/07/ha-ha-ha-ha-ha-riaa-paid-its-lawyers.html Accessed 05/03/21 **Note: This cites p2p.net documents as the root source, this site was shut down however these documents can be accessed through the wayback machine if you wanted to view the raw income forms.**

Orlowski, A (2005) *RIAA Sues the dead* The Register, 5 Feb, https://www.theregister.com/2005/02/05/riaa_sues_the_dead/ Accessed 05/02/21

British Phonographic Industry (2020) *BPI sends 500 millionth illegal link to Google for removal from search results,* https://www.bpi.co.uk/news-analysis/bpi-sends-500-millionth-illegal-link-to-google-for-removal-from-search-results/ Accessed 05/02/21

UK Government (2017) *Code of practice on search and copyright* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609478/code-of-practice-on-search-and-copyright.pdf Accessed 05/02/21

ISPreview (2019) *BPI Reveal UK Broadband ISPs Have Sent 1 Million Privacy Alert Emails* https://www.ispreview.co.uk/index.php/2019/02/bpi-reveal-uk-broadband-isps-have-sent-1-million-piracy-alert-emails.html Accessed 06/02/21

European Digital Rghts (2012) *The Digital Millennium Copyright Act (DMCA) as a model?* https://edri.org/files/0409_annex_unintcons.pdf Accessed 05/02/21

Malicious Communications

What is Malicious Communication?

A malicious communication is described in British law as any letter, electronic communication or article of any description sent with the intent to cause distress or anxiety.

UK Government Legislation, no date A

The intent of the message and the mental state of the sender are very important in deciding whether or not any message is malicious.

Malicious Communication Offences - JMW Solicitors, no date

Laws that apply in the UK

Malicious Communications Act 1988

Makes it an offence to send another person a communication in any form which is indecent, grossly offensive, a threat, or knowably false.

UK Government Legislation, no date A (Section 1)

Communications Act 2003

The Communications Act covers public electronic communications and makes it an offence to send grossly offensive, indecent or obscene messages, or messages of menacing character.

UK Government Legislation, no date B (Section 127)

How does the US compare?

The US is a much different story because of their 1st Amendment. This means they have a much more lenient approach to what is malicious, limiting it more to threats to commit crimes such as extortion or kidnap.

Cornell Law School (no date A&B)

The US also have the Communications Decency Act (1996), which makes it an offence to transmit obscene or indecent materials over the internet. This act is specifically related to pornographic content.

Thomson Reuters Practical Law (no date)

Appropriateness Of UK Law

Compared with US laws, the UK’s laws cover much more ground.

Where the US law is only related to threats to commit other crimes, the UK have provisions for distribution of false information or the causing of distress and anxiety.

UK Government Legislation, no date A

The UK laws seem much more fit for purpose, when compared with those of the US.

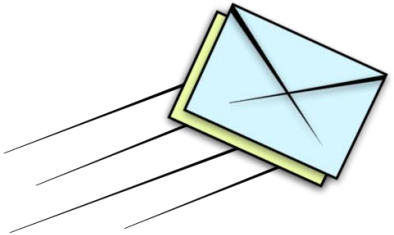
Example of Malicious Communications Act 1988 in use

In 2005, an anti-abortion campaigner was convicted for sending “offensive” pictures of aborted foetuses to chemists who sold the morning-after pill.

Veronica Connolly admitted to sending the photos, but argued that they were not offensive or indecent in nature.

She was given a 12 month conditional discharge and ordered to pay legal fees.

BBC News (23/01/2007)



References (in order of use)

UK Government Legislation (no date A) Malicious Communications Act 1988 https://www.legislation.gov.uk/ukpga/1988/27 Accessed 06/02/2021

JMW Solicitors (no date) Malicious Communications Offences https://www.jmw.co.uk/services-for-business/business-crime/malicious-communications-act-offences Accessed 06/02/2021

UK Government Legislation (no date B) Communications Act 2003 https://www.legislation.gov.uk/ukpga/2003/21/part/2/chapter/1/crossheading/offences-relating-to-networks-and-services Accessed 07/02/2021

Cornell Law School (no date A) 18 U.S. Code § 875 - Interstate communications https://www.law.cornell.edu/uscode/text/18/875 Accessed 08/02/21

Cornell Law School (no date B) 18 U.S. Code § 876 - Mailing threatening communications https://www.law.cornell.edu/uscode/text/18/876 Accessed 08/02/2021

Thomson Reuters Practical Law (no date) Communications Decency Act of 1996 (CDA) https://uk.practicallaw.thomsonreuters.com/9-502-8947?transitionType=Default&contextData=(sc.Default)&firstPage=true Accessed 08/02/2021

BBC News (23/01/2007) Rights case over foetus pictures http://news.bbc.co.uk/1/hi/england/west_midlands/6291653.stm Accessed 08/02/2021

Data Theft

UK: Data Protection Act 2018

- The UK’s implementation of GDPR
- All people or organizations who store and handle personal data must follow “data protection principles”
- A person has the right under the act to know what information is stored about them

(Data protection, n.d.)

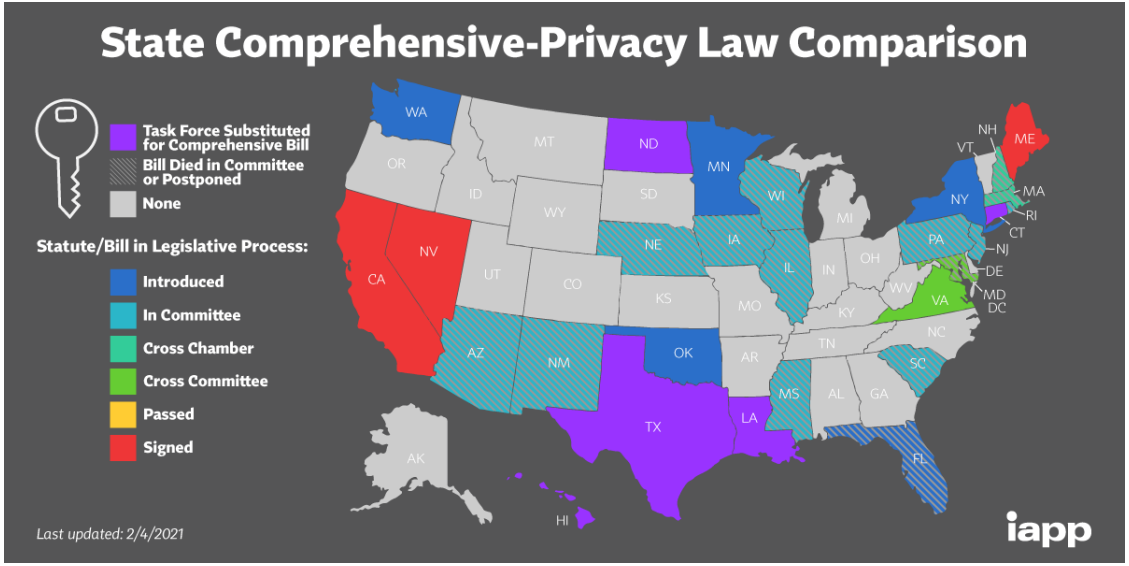
- Revision of the Data Protection Act (1998)
- Right to erasure
- Makes exemptions clear

(Data Protection Act 1998 - Be Compliant | Seers, n.d.)

US: Multiple laws

- The US Privacy Act of 1974 covers data collected by federal agencies
- Prevents disclosure of data without written permission
- There are state laws in California, Nevada, and Maine

(Complete Guide to Privacy Laws in the US | Varonis, 2020)



(US State Comprehensive Privacy Law Comparison, 2021)

State laws

California

California Consumer Privacy Act (CCPA)

- Right to know about data stored
- Right to delete data
- Right to opt out of the sale of data
- Cannot be discriminated against for exercising rights

(California Consumer Privacy Act (CCPA), n.d.)

Nevada

Senate Bill 220

- Right to opt out of sale of data
- No rights for accessing or deleting data
- No right to non-discrimination

(The Nevada Privacy Law vs. The CCPA | OneTrust Blog, 2019)

Maine

Act to Protect the Privacy of Online Customer Information

- Focuses on ISPs
- Opt in consent to sale
- Opt out of sharing of non-personal information
- Right to non-discrimination

(Maine Privacy Law: What's the Impact? | RampUp, 2019)

Which is more appropriate?

Overall, UK law seems most appropriate. US federal law only covers federal agencies, and the majority of states do not yet have active data protection laws, although many are in the process of creating them. This means that, unless you are in one of the 3 states with data privacy laws, you essentially have no protection.

Out of the 3 states that do have data protection laws, California's is the most appropriate, with Maine as a close second. Both states provide strong rights around data protection, and allow people to exercise their rights without being denied service for it. Nevada state law provides almost no protection, and allows service providers to discriminate against people who do not want their data sold.

Example: British Airways data breach

In 2018, British Airways had a data breach where their customers were redirected to a fraudulent site designed to steal personal information. The incident is thought to have affected approximately 500,000 passengers. Details such as emails, addresses, and credit card information was leaked.

British airways were fined £183 million for the incident.

(British Airways faces record £183m fine for data breach, 2019)

References

GOV.UK. n.d. Data protection. [online] Available at: <https://www.gov.uk/data-protection> [Accessed 8 February 2021].

Iapp.org. 2021. US State Comprehensive Privacy Law Comparison. [online] Available at: <https://iapp.org/resources/article/state-comparison-table/> [Accessed 8 February 2021].

Inside Out Security. 2020. Complete Guide to Privacy Laws in the US | Varonis. [online] Available at: <https://www.varonis.com/blog/us-privacy-laws/> [Accessed 8 February 2021].

Justice.gov. 2015. Overview of the Privacy Act of 1974. [online] Available at: <https://www.justice.gov/opcl/conditions-disclosure-third-parties> [Accessed 8 February 2021].

OneTrust. 2019. The Nevada Privacy Law vs. The CCPA | OneTrust Blog. [online] Available at: <https://www.onetrust.com/blog/the-nevada-privacy-law-sb-220-vs-the-california-consumer-privacy-act-ccpa/> [Accessed 8 February 2021].

References

RampUp. 2019. Maine Privacy Law: What's the Impact? | RampUp. [online] Available at: <https://rampedup.us/maine-privacy-law-impact/#:~:text=On%20July%201%2C%202020%2C%20Maine,Internet%20Service%20Providers%20(ISPs).> [Accessed 8 February 2021].

Seers | Articles. n.d. Data Protection Act 1998 - Be Compliant | Seers. [online] Available at: <https://seersco.com/articles/data-protection-act-2018-vs-data-protection-act-1998/> [Accessed 8 February 2021].

State of California - Department of Justice - Office of the Attorney General. n.d. California Consumer Privacy Act (CCPA). [online] Available at: <https://oag.ca.gov/privacy/ccpa#:~:text=The%20California%20Consumer%20Privacy%20Act,rights%20for%20California%20consumers%2C%20including%3A&text=The%20right%20to%20opt%2Dout,of%20their%20personal%20information%3B%20and> [Accessed 8 February 2021].

BBC News. 2019. British Airways faces record £183m fine for data breach. [online] Available at: <https://www.bbc.co.uk/news/business-48905907> [Accessed 8 February 2021].

Malware

Definition of malware in law

- The US defines malware as “software designed to destroy, damage, disable, or gain unauthorized access to any computer system, software, or electronic data” (1).
- The UK considers malware to be a “cyber-dependent crime”. Malware is categorized under “the disruption or downgrading of computer functionality and network space” (2). An example of this being “developing and propagating malware for financial gain” (2).

Relevant UK laws

The Computer Misuse Act 1990 (CMA)

- Section 3 prohibits “unauthorized acts with intent to impair, or with recklessness as to impairing, operation of computer” . Maximum 10 years of imprisonment (3).

The Fraud Act 2006

- Section 7 means making malware can be considered an offence if the malware was used or intended to be used to commit fraud. Maximum 10 years of imprisonment (4).
- Section 6 can also apply to malware. Maximum 5 years of imprisonment (4).

Relevant US laws

Computer Fraud and Abuse Act of 1986 (CFAA)

- “Causing damages ... by knowingly transmitting harmful items or intentionally accessing a protected computer”. This would include planting of malware. The maximum penalty is 10 years of imprisonment (5).
- Subsection (5)(A) prohibits anyone from intentionally damaging a computer (without authorization).

Appropriateness

- In the US, the definition of a "protected computer" has been broadened to mean essentially any computer (6). The CFAA prohibits unauthorized access to protected computers alongside federal government computers.
- The CMA and the CFAA both implement the idea of “intentional” unauthorized access.

Marcus Hutchins

- UK cyber security researcher Marcus Hutchins was responsible for finding a kill switch to the WannaCry ransomware.
- After his arrest for suspected development of the malware “Kronos”, he said “this could very easily be the FBI mistaking legitimate research activity with being in control of Kronos infrastructure” (7).
- The judge viewed Marcus as a cyber security expert who had “turned the corner”. “There are just too many positives on the other side of the ledger” (8).

References

- 1 - https://uk.practicallaw.thomsonreuters.com/2-502-5221
- 2 - https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance
- 3 - https://www.legislation.gov.uk/ukpga/1990/18/contents
- 4 - https://www.legislation.gov.uk/ukpga/2006/35/contents
- 5 - https://uk.practicallaw.thomsonreuters.com/2-508-3428
- 6 - https://www.cybersecurityeducationguides.org/what-is-the-computer-fraud-and-abuse-act/
- 8 - https://www.theguardian.com/technology/2017/aug/03/researcher-who-stopped-wannacry-ransomware-detained-in-us
- 7 - https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/