Chapter 5
Regulating the Internet—Necessary Evil or Squandered Opportunity?

Ruth Barber

Introduction

The birth of the Internet heralded a potential new world of freedom for trade and expression, and free from governmental interference, a fundamentally U.S. libertarian worldview. As the Internet moved from a U.S. based online community of technical enthusiasts to become a global communication network, attempts were made to regulate cyberspace by competing commercial, security and moral interests. Governments attempted to assert control through technical and regulatory measures. Control measures imposed include geo-blocking, ISP regulation and hardware control (China), the repeal of Net Neutrality rules (USA), the Network Enforcement Act (Germany) and the General Data Protection Regulation (EU).

However, the global and networked nature of the Internet makes it inherently resistant to geographical control, and regulatory measures imposed tend to result in jurisdictional overreach. How then should the Internet be regulated, assuming that regulation is now deemed necessary? Cyberspace is increasingly dominated by a few transnational platform providers. Is the regulation of the Internet now effectively controlled by these organizations, whose economic power and political influence exceeds the power of many nation states? If so, has the Internet become the independent jurisdiction that its early creators dreamed it should be?

R. Barber (✉)
London, Great Britain
e-mail: ruth.barber@ruthbarberconsulting.co.uk

Berlin, Germany

D. Feldner (ed.), *Redesigning Organizations*,
https://doi.org/10.1007/978-3-030-27957-8_5

The Information Sharing Revolution

The development of the Internet has enabled an information sharing revolution. Ordinary citizens can now bypass the publishing houses that previously controlled information sharing. Citizens have the independent power to share information quickly and cheaply with millions of other people throughout the globe.

The information sharing phenomena took off via social media platforms such as Facebook, YouTube and Twitter. These sites are designed to facilitate information sharing to maximize user engagement. They do not charge a fee for their use but are funded by advertising revenue. Maximum user engagement means maximum advertising revenue. The more information the sites have about their users, the better the advertising can be targeted. Cambridge Analytica, a political advertising company, harvested millions of Facebook users' data through a third-party application in order to better target political advertising (Cadwalladr and Graham-Harrison 2018).

Social networking sites claim to be information sharing platforms rather than publishers, and therefore exempt from defamation laws (Jarvis 2018; Kiss and Arthur 2013; House of Lords 2018). The European eCommerce Directive 2000/31/EC Article 12 provides a liability exemption for online information hosts providing they have no prior knowledge of unlawful activity and act quickly to remove the offending material when notified. This provision is mirrored in the U.S. in section 230 of the Communication Decency Act.

Social networking platforms claim to exercise no editorial control over content published save via their community guidelines (Facebook 2018), which filter for obscene and violent content. The platforms do control what material appears in a user's news feed by use of an algorithm, periodically tweaked (Peters 2018). Facebook has admitted to experimenting on groups of users by deliberately manipulating the material appearing in their news feeds. The use of this algorithm weakens Facebook's assertion that it is a mere information conduit.

A 2018 court case has eroded Facebook's claim to be a mere information sharing platform. Martin Lewis, a British champion for consumer rights, sued Facebook when his image was appropriated without consent for advertising on Facebook. He argued that since he does not engage in Facebook advertising, it should be a simple matter for Facebook to remove every advert with his image without the need for him to report the advertisements. However, advertising is not third-party content, and the court held Facebook jointly liable (FT 2018).

As Facebook gets increasingly hit with lawsuits, it appears to now be willing to define itself as a publisher in order to take advantage of the first amendment of the US Constitution protection for publishers, which protects free speech. It still seems unfair to hold social media platforms, who are not editors, liable for user postings. It may be that historical terms such as "publisher" are no longer adequate to describe the modern media landscape and the scope of legal liability (Levin 2018).

Social Networks and Psychology

The social network business model has a number of unfortunate social effects. Profit is made from users responding to and sharing information, and human nature tends to respond automatically to information that surprises, shocks or offends. Since no control on social media is made for truth, profitable "fake news" proliferates. Much of this fake news is generated by individuals with no agenda other than to make money (Ball 2017).

Nefarious actors have also realized the potential for spreading political propaganda. Russia established troll farms for the purpose of spreading disinformation on social media sites and generating social unrest in the West (Green 2018). The development of "deep fake", an AI driven application, allows for digital impersonation and the production of convincing videos of people of doing and saying things they never did (Chesney and Citron 2018).

Rather than presenting a range of views that might challenge or inform, social networking sites give us more of what we like. This has the effect of reinforcing and entrenching existing views. It is alleged that the use of "fake news" had an influence on both the Brexit Vote and the U.S. presidential election in 2016 (Fiadh 2017).

When challenged, the response of social networking sites has been reluctant and ineffectual (Hill 2018). Their business models rely on the maximum amount of user engagement, both in terms of time and number of participants.

States that were previously keen to court the social networking companies with favorable tax rates have become increasingly hostile (Cadwalladr 2018). Users are also becoming increasingly disillusioned and are leaving the platforms and sharing less personal information (Locklear 2018).

Concern about user disengagement as a result of privacy concerns has resulted in greater efforts by social networking sites to demonstrate privacy protections. However, a business model that is predicated on harvesting data for profit is arguably always vulnerable to abuse. A subscription model would remove the reliance on advertising revenue, but it would also discourage many users, reducing market share.

A Borderless Internet?

> Governments cannot stop electronic communications from coming across their borders, even if they wanted to do so. Nor can they credibly claim a right to regulate the Net based on supposed local harms caused by activities that originate outside their borders and that travel electronically to many different nations. One nation's legal institutions should not monopolize rule-making for the entire Net. Even so, established authorities will likely to continue to claim that that they must analyze and regulate the new online phenomena in terms of physical locations. After all, they argue, people engaged in online communications still inhabit the material world, and local legal authorities must have authority to remedy the problems created in the physical world by those acting on the Net. (Johnson and Post 1996)

The prophesy of Johnson and Post is illustrated in the cases of LICRA and UEJF v. Yahoo! and Microsoft Corp v. United States. Both attempt to exert extraterritorial jurisdiction to the Internet. In LICRA and UEJF v. Yahoo!, attempts are made to regulate a U.S. website visible in France. In the Microsoft case, the question relates to a U.S. company storing information "in the cloud" but using a Dublin-based server.

LICRA and UEJF v. Yahoo! Inc

French users of the Yahoo! online auction site were able to view and purchase Nazi memorabilia. The offering of Nazi memorabilia for sale is prohibited in France. The League against racism and antisemitism and the Union of French Jewish Students brought a case against Yahoo! Inc. in France. The French court found a sufficient nexus to establish jurisdiction, since the items were viewable by French citizens and this was known to Yahoo! Inc., since they targeted French users with French advertising. Yahoo! Inc. had a French subsidiary, Société Yahoo! France.

The French court found in favor of the applicants and ordered Yahoo! to block Nazi memorabilia from French citizens. Yahoo! resisted the order and attempted to argue that selective blocking of French users was impossible; experts disputed the claim and argued that 90% blocking was possible. The court required Yahoo! to impose the blocking or be subject to fines of 15,244 Euros per day.

Yahoo! then filed a case against the applicants in a U.S. court (the District Court for the Northern District of California), arguing that the French decision was not binding upon them in the U.S. The applicants argued that any finding of the U.S. court was not binding on them in France.

The U.S. court stated, "A basic function of a sovereign state is to determine by law what forms of speech and conduct are acceptable within its borders". The issue was "whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a U.S. resident on the basis that such speech can be accessed by Internet users in that nation" (LICRA v. Yahoo!). Yahoo!'s application was granted. LICRA appealed and the decision was reversed on the basis that the District Court did not have jurisdiction over LICRA.

Judge William Fletcher stated in a judgement on 12 January 2006:

> Yahoo! is necessarily arguing that it has a First Amendment right to violate French criminal law and to facilitate the violation of French criminal law by others. […] the extent — indeed the very existence — of such an extraterritorial right under the First Amendment is uncertain.

Following the judgement, Yahoo! elected to remove all Nazi memorabilia from its site.

Ultimately, Yahoo! Inc. was obliged to comply with the French judgement as a result of its economic interests in France. Businesses that have no economic interests in a country cannot be regulated so easily by legal means.

Microsoft Corp. v. United States

In 2013, Microsoft challenged a warrant issued under section 2703 of the Stored Communications Act (SCA) by the U.S. federal government to turn over the emails of an account that was stored in Ireland (Microsoft v. U.S.). It argued that the Act could not be used to compel American companies to produce data stored in servers outside the U.S. The judge at first instance found against Microsoft on the basis that the Act was not subject to territorial restrictions. The Irish government filed a brief in the proceedings, arguing that the decision violated the European Data Protection Directive and Ireland's data privacy laws. Ireland argued that the emails could only be disclosed on request to the Irish Government. Microsoft won on appeal, with the court holding that legislation only has national effects unless it is clearly expressed to the contrary. The warrant also did not specify whether the owner of the emails was a U.S. citizen or resident. The Department of Justice appealed to the Supreme Court.

While the Supreme Court hearing was pending, Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which amended the SCA to specifically include cloud storage of U.S. providers, regardless of where the servers may be located. This act was supported by both the U.S. Government and Microsoft. The Supreme Court hearing was then moot, and the appeal court hearing vacated.

China

China realized the limited options for exercising legal control over U.S. providers of information technology that have no significant assets in the country, and instead developed indigenous versions of Google and Facebook products, which come preloaded on smartphones sold in China. The Chinese government has a monopoly on all national internet connections via the Ministry of Information Industry (MII). The number of ISPs is restricted, and each provider must be approved by the MII. ISPs are required to block websites named by the Public Security Bureau. In addition, the authorities monitor and control all traffic going through China's primary gateways to the global Internet (Chew 2018).

Compared to the U.S.—with its emphasis on freedom of expression embodied in the First Amendment—the Chinese approach is arguably restrictive and repressive. However, the right to freedom of expression is upheld in the U.S. at the expense of personal privacy, which in the U.S. has only minimal legal protection.

Germany

The Snowden revelations of 2013 revealed the extent of U.S. online intelligence operations that routinely harvest the data of users of U.S. based information technology services (Macaskill and Dance 2013). A backlash against U.S. information services occurred in Germany, when it was discovered that U.S. intelligence services had eavesdropped on the private telephone calls of Angela Merkel. Germans, who have a particular cultural sensitivity to personal data harvesting due to data abuses undertaken by the Nazi regime (Freude and Freude 2016), increasingly moved to onshore their data and transfer to national information service providers (Spiegel 2013).

Germany, long a champion of European privacy rights, also pushed for the enactment of the General Data Protection Regulation, which provides for strong privacy protections for European Citizens. The regulation also recognized the global effects of the web and the need to be able to enforce against businesses with neither a legal or a physical presence within the EU jurisdiction. Article 3(2) allows the application of the EU Regulation to non-EU based data processors that process the data of individuals in the EU in two situations: first, if they are offering goods and services in the EU; and second, if they are monitoring of the behavior of people in the EU.

"The Regulation amounts to a unilateral expansion of the application of European law to non-EU businesses. No one could deny that this expansion is justified by the borderless domain of the Internet, which in response requires also a borderless application of the law. In a way, there is no doubt that effective data protection on the Internet does not get along with a domestic scope of application. Nonetheless, the EU dares to go much further than any other state on this aspect, and with the highest level of standards in the world" (Azzi 2018). Effective enforcement is still largely reliant upon the companies having enough economic or political nexus with the EU.

Having seen the problems that arose from alleged online electoral interference in the UK referendum and the U.S. election and fighting battles against the rise of right-wing extremism that flourished on social networking sites, Germany pushed through the controversial Network Enforcement Act on 1 October 2017. This Act placed a legal obligation on large social networking platforms to remove content that offended specific provisions of the German Criminal Code or be subject to swinging fines. The Act was criticized by free speech champions also for its extraterritorial effect (Jash 2017). Complaints can only be made under the Act "in Germany", but targeted material may come from any jurisdiction.

United States of America

On 14 December 2017, the U.S. Federal Communications Commission voted to repeal Net Neutrality. Net Neutrality is the principle that internet service providers treat all data on the internet equally and do not discriminate or charge

differently by user, content, website, platform, application, type of attached equipment or method of communication (Gilroy Gilroy 2011). The basis for the decision was to increase competition (Selyukh and Greene 2017), however, critics argue that the repeal of Net Neutrality permits government censorship (Skorup 2016) as it permits the preferential online delivery of, for example, government approved news channels. Twenty-two U.S. states are appealing against the ruling and a hearing is due in February 2019.

Legal Measures

Civil legal measures are only effective in so far as the regulated entity has assets in the jurisdiction of the complainant, or to the extent that judgements in one jurisdiction are enforceable in another. Countries with close political and trading arrangements may choose to honor judgements.

Online criminal enforcement is only possible between sympathetic jurisdictions with similar criminal law standards. A website removed in one country under a notice and take down procedure, can simply reappear hosted on a server in a more libertarian or sympathetic jurisdiction.

Some alt-right groups purged from Facebook and Twitter have joined the Russian Facebook clone VKontakte (Zavadksi 2017), which has greater tolerance for white supremacist views. Jihadi groups joined the encrypted social networking site Telegram. Some pornographic and holocaust denial websites taken down from European servers have found a home in the U.S.

Technical Measures

Geo-blocking—i.e., restricting Internet access based on a user's supposed location—can be thwarted by the use of a proxy server. Surveillance of online activity can be thwarted by the use of a VPN (Virtual Private Network), which encrypts internet traffic. Platforms and electronic service providers are however becoming increasingly aware of these techniques and are developing responses to combat them.

Search engine results can be manipulated to produce no results in certain jurisdictions in response to regulated search terms. This raises questions of censorship and is likely to deter only passive or naïve searchers.

Internet traffic can be filtered on the basis of restricted key words or site blacklists. This method frequently results in incorrect blocking or overblocking. This is a method used by the industry-led Internet Watch Foundation, which has successfully reduced the amount of child pornography hosted in the UK, although this material has frequently reappeared in another jurisdiction.

The global nature of the internet means that jurisdictional efforts to regulate online content and behavior are likely to deter only the most passive or naïve. This may help

to prevent influencing from foreign political propaganda but will do little to prevent the determined and technologically savvy from accessing information.

The Dark Net

The Dark Net is the part of the Internet not open to public view and only accessible using the Tor browser, which permits anonymized browsing. It contains websites and file locations that are not indexed by conventional search engines and are, therefore, hard to find. Criminals and extremists can avoid monitoring by using a series of "redirects": links that must be followed by invited users to reach certain sites. If content is not indexed by search engines, it is not possible for regulators to tweak search results to hide it. If its location is not known, filtering with reference to blacklists will not work, as the material will not make it onto these lists in the first place. If authorities cannot locate content, they cannot attempt to remove it (Stevens 2009).

The anonymity afforded to users of the Dark Web provides safe internet access for criminals but also for investigative journalists and users blocked from accessing information by repressive regimes.

The Dark Web continues to act as a marketplace for the exchange of illegal goods and services, notwithstanding the shutting down of its infamous Silk Road marketplace and the imprisonment of its founder, Ross Ulbricht, in the U.S. in 2013. The investigation and action by the FBI were intended to send a message that even the Dark Web was not outside the control of U.S. law enforcement.

Payment for goods on the site was made by the untraceable cryptocurrency Bitcoin. Ulbricht created the marketplace to function without government oversight but found it difficult to verify anonymous transactions, since the anonymity afforded to buyers and sellers prevented relationships of trust from being established. Ironically, scammers complained about being scammed, since anonymity precluded accountability. Ulbricht started increasing oversight. He added measures to ensure trustworthiness with implementation of an automated escrow payment system and automated trader review system similar to the features of the Amazon legal online trading platform. As the site became increasingly profitable, Ulbricht suffered threats from the traders. In the absence of state mechanisms for enforcement, he allegedly sought to hire thugs to enforce his business (Farrell 2015).

In a letter to the judge before his sentencing, Ulbricht stated that his actions via Silk Road were committed through libertarian idealism and that "Silk Road was supposed to be about giving people the freedom to make their own choices" (Snyder 2015). Unfortunately, giving people the freedom to make their own choices meant they made choices in their own interest to his detriment. His experiment in creating an online libertarian utopia was ultimately a failure. In the words of Robert Lee Hale "There is government whenever one person or group can tell another what to do, and when those others have to obey or suffer a penalty" (Samuels 1992).

Accountability is a necessary feature of a functioning online community. The question is whether this accountability can only be provided by nation state based systems.

The primarily illegal nature of the goods on the Silk Road site meant that traders and purchasers were uniquely vulnerable. But what if Ulbricht had been selling lawful goods? Such a business model exists and is wildly successful.

Amazon.com

Amazon is a U.S. based global electronic trading platform, operating with national subsidiary websites throughout the world. Traders register with the site and supply goods to customers who log in with a password and email. Amazon does not verify the traders beyond basic identifying details, but a trust system is in operation where customers can rate the traders. The company offers its own escrow system and takes a fee from the seller for every transaction. Anyone in the world can sell to anyone in the world on the site (save in countries where is the service is blocked). The national subsidiary sites cater to national markets, but there is no block on, say, a UK user buying from the U.S. site, although national restrictions may block the purchase of certain goods.

It is no accident that the trading model of Amazon and Silk Road are almost identical, since they have evolved to make the most efficient use of the architecture of the Internet. Amazon recognizes national jurisdictions through its subsidiaries but ultimately still provides a global trading platform. It ensures accountability deliverable though its own dispute resolution system.

As national jurisdictions struggle to regulate the global nature of the Internet, it seems that transnational global service providers are filling the gap. We are seeing the rise of "Corporation as Courthouse" (Van Loo 2016).

Just as Amazon can now exercise jurisdiction over online trade disputes, Facebook can exercise jurisdiction over online expression. After many years of holding out, Facebook has increased the strictness and enforcement of its "community guidelines" in the face of national regulation. These standards are public and of global application. Facebook even offers its own appeals process (Newton 2018).

The loss of territorial sovereignty is being replaced with functional sovereignty (Pasquale 2017). It may be more efficient, but as the power of the platforms grows relative to national power, how are the platforms themselves to be held accountable? Are we entering a neo-feudal arrangement where the power to obtain "justice" is not based on the rule of law but on an individual's economic leverage on the platform? Or have the platforms already become so powerful and ubiquitous that they are effectively a digital public space, wielding the ultimate sanction of digital social exclusion against recalcitrants?

Conclusion

> Many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct place for purposes of legal analysis … What procedures are best suited to the often-unique characteristics of this new place and the expectations of those who are engaged in various activities there? What mechanisms exist or need to be developed to determine the content of those rules and mechanisms by which they can be enforced? Answers to those questions will permit the development of rules better suited to the new phenomena in question, more likely to be made by those who understand and participate in those phenomena, and more likely to be enforced by means that the new global communications media make available and effective. (Johnson and Post 1996)

Libertarians have discovered that the borderless nature of the Internet is the perfect architecture for the market, rather than nation states (Boushey 2017). This model is expanding across the globe via the rise of multinational service providers and fits the model of regulating cyberspace as a separate entity, proposed by Johnson and Post. China has resisted, but only through the use of pervasive technological blocking techniques. Does the rise of the Net mean that future regulation of citizens is now polarized between market forces or absolute state control? Or can democracy evolve to regulate the Internet (Schlechtman 2018)?

References

Articles

Azzi, A. (2018). The challenges faced by the extraterritorial scope of the general data protection regulation. *JIPITEC 9*, 126 para 30.

Johnson, D. R., & Post, D. G. (1996). Law and borders—The rise of law in cyberspace. *Stanford Law Review, 48*, 1367, 1378–1379, 1390–1391.

Pasquale, F. (2017, December 6). From territorial to functional sovereignty: The case of Amazon. *Law and Political Economy*. https://lpeblog.org/2017/12/06/from-territorial-to-functional-sovereignty-the-case-of-amazon/.

Samuels, W. J. (1992). *Essays in the history of Heterodox Political Economy* (p. 184). Macmillian.

Stevens, T. (2009, April). *RUSI Journal, 154*(2), 28–33.

Van Loo, R. (2016). The corporation as courthouse. *Yale Journal on Reg, 33*.

Books

Ball, J. (2017). *Post-truth: How bullshit conquered the world*.

Judgements

"LICRA et UEJF v. Yahoo! Inc and Yahoo! France" Tribunal de Grande Instance de Paris, 22 May 2000.
United States v. Microsoft Corporation, Supreme Court of the United States 584 U.S.__ 2018.

Laws

Cloud Act, H.R. 4943—Clarifying Lawful Overseas Use of Data Act, 23 March 2018. https://nsarchive.gwu.edu/news/cybervault/2018-04-02/hr-4943-clarifying-lawful-overseas-use-data-act-cloud-actMedia.
Network Enforcement Act. https://germanlawarchive.iuscomp.org/?p=1245.

Media

Boushey, H. (2017, August 15). How the radical right played the long game and won. *New York Times*. https://www.nytimes.com/2017/08/15/books/review/democracy-in-chains-nancy-maclean.html.
Cadwalladr, C. (2018, November 24). Parliament seizes cache of Facebooks internal papers. *The Guardian*. https://www.theguardian.com/technology/2018/nov/24/mps-seize-cache-facebook-internal-papers.
Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool. *The Guardian*. https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm.
Farrell, H. (2015, February 20). Dark Leviathan. *Aeon Essays*. https://aeon.co/essays/why-the-hidden-Internet-can-t-be-a-libertarian-paradise.
Fiadh, M. (2017, December 18). The dangers of echo chambers, complacency, and fake news. *The Irish Times*. https://www.irishtimes.com/student-hub/the-dangers-of-echo-chambers-complacency-and-fake-news-1.3331458.
Green, J. J. (2018, September 17). Tale of a troll: Inside the 'Internet Research Agency' in Russia. *Washington's Top News*. https://wtop.com/j-j-green-national/2018/09/tale-of-a-troll-inside-the-Internet-research-agency-in-russia/.
Hill, A. (2018, March 19). Facebook's floundering response to scandal is part of the problem. *The Financial Times*. https://www.ft.com/content/42491a80-2b5b-11e8-a34a-7e7563b0b0f4.
Jarvis, J. (2018, August 10). Platforms are not publishers. *The Atlantic*. https://www.theatlantic.com/ideas/archive/2018/08/the-messy-democratizing-beauty-of-the-Internet/567194/.
Kiss, J., & Arthur, C. (2013, July 29). Publishers or platforms? Media giants may be forced to choose. *The Guardian*. https://www.theguardian.com/technology/2013/jul/29/twitter-urged-responsible-online-abuse.
Levin, S. (2018, July 2). Is Facebook a publisher? In public it says no, but in court it says yes. *The Guardian*. https://www.theguardian.com/technology/2018/jul/02/facebook-mark-zuckerberg-platform-publisher-lawsuit.
Macaskill, E., & Dance, G. (2013, November 1). NSA FILES: DECODED. *The Guardian*. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

Newton, C. (2018, April 24). Facebook makes its community guidelines public and introduces an appeals process. *The Verge*. https://www.theverge.com/2018/4/24/17270910/facebook-community-guidelines-appeals-process.
Selyukh, A. & Greene, D. (2017, May 5). FCC chief makes case for tackling net neutrality violations 'After The Fact'. *National Public Radio.* https://www.npr.org/sections/alltechconsidered/2017/05/05/526916610/fcc-chief-net-neutrality-rules-treating-Internet-as-utility-stifle-growth?t=1543780680159.
Spiegel Online. (2013, August 26). *German email services report surge in Demand*. http://www.spiegel.de/international/germany/growing-demand-for-german-email-providers-after-nsa-scandal-a-918651.html.
Schlechtman, J. (2018, April 13). *The internet is killing democracy, whowhatwhy.org.* https://whowhatwhy.org/2018/04/13/the-Internet-is-killing-democracy/.
Skorup, B. (2016, June 20). Net neutrality is government censorship. *National Review*. https://www.nationalreview.com/2016/06/net-neutrality-government-control/.
Snyder, B. (2015, May 27). Silk Road mastermind pleads for light sentence. *Fortune*. http://fortune.com/2015/05/27/silk-road-sentencing/.
"In online advertising, Facebook is a publisher," *The Financial Times*, April 23, 2018. https://www.ft.com/content/9206f5f2-46f8-11e8-8ee8-cae73aab7ccb.
Zavadski, K. (2017, November 3). American Alt-Right Leaves Facebook for Russian Site VKontakte. *The Daily Beast*. https://www.thedailybeast.com/american-alt-right-leaves-facebook-for-russian-site-vkontakte.

Studies and Guidance

Congressional Research Service, & Gilroy, A. A. (2011, March 11). *Access to broadband networks: The net neutrality debate* (Report) (pg. 1). DIANE Publishing. ISBN: 978-1437984545.
Freude, A., & Freude, T. (2016, October 1). *Echoes of history: Understanding German data protection, Bertelsmann Foundation*. https://www.bfna.org/research/echos-of-history-understanding-german-data-protection/.
House of Lords Library Briefing (2018, January 8). *Social media and online platforms as publishers*. https://researchbriefings.parliament.uk/ResearchBriefing/Summary/LLN-2018-0003.

Web References

Amazon Buyer Dispute Program. https://pay.amazon.com/us/help/201751580.
Chesney, R., & Citron, D. (2018, February 21). Deep fakes: A looming crisis for national security, democracy and privacy? LAWFARE Blog.
Chew, W. C. (2018, May 1). How it works: Great firewall of China. https://medium.com/@chewweichun/how-it-works-great-firewall-of-china-c0ef16454475.
Facebook Community Standards. (2018). https://www.facebook.com/communitystandards/.
Peters, B. (2018, February 8). The new Facebook algorithm: Secrets behind how it works and what you can do to succeed. Buffer Social Blog. https://blog.bufferapp.com/facebook-algorithm.
Locklear, M. (2018, September 5). Facebook users are changing their social habits amid privacy concerns. *Engadget*. https://www.engadget.com/2018/09/05/facebook-changing-social-habits-privacy-concerns/?guccounter=1.

Jash, S. (October 27, 2017). *Outsourcing censorship, attacking civil liberties: Germany's NetzDG*. https://www.hertie-school.org/the-governance-post/2017/10/outsourcing-censorship-attacking-civil-liberties-germanys-netzdg/.

Yahoo! Inc v LICRA and UEJF No. 01-17424 United States Court of Appeals for the 9th Circuit 443 433 F.3d 1199 (9th Cir. 2006)

Ruth Barber is currently completing a Master's Degree in IT and Communications Law with Queen Mary University London and researching the regulation of social media. She completed a law degree in 1995, was admitted to the Bar of England and Wales in 1996 and became a Solicitor (England and Wales) in 1998. She gained Higher Rights of Audience in 2005. She was admitted to the UK Attorney General's list of Counsel in 2007 and was shortlisted for Solicitor Advocate of the Year in 2010. She specializes in regulatory criminal law and works as an international legal consultant. Ruth is the co-author of the Confiscation Law Handbook 2011, published by Bloomsbury Professional.