Shared Internet Connections Within the Residential Sphere: Achieving a Safer and Clearer Implementation

Table of Contents:

6.2. Rethinking Liability

6.3. Copyright

6.4. Unnecessary Technology

Conclusion

Bibliography

Abstract

The unnecessary difficulty currently surrounding establishing a shared internet connection is testament to a series of misinformed legislative choices and policy norms which are hindering society from greater access to the internet. This paper is an examination of the current risks surrounding sharing one's residential internet connection and a series of policy recommendations available for helping to overcome these risks. The suggestions offered within this paper will largely be targeted at legislators. This can be accounted to the fact that many of the problems present require a legislative resolution. Alongside this, advocacy of higher technical standards and security as a requirement for router technology and web pages will be forwarded. Although these will be targeted at legislators, they could also be independently implemented by other stakeholders such as internet access providers and the developers of routers. It is hoped that the suggestions offered in the paper will bolster security, whilst also increasing clarity on a topic which is often unfairly stigmatised. Such a strategy would benefit both consumers and businesses within Europe in a number of ways, and could be perceived as an extra crucial facet to a more complete European Digital Single Market.

Introduction

Over the past decade there has been an extensive growth in the number of people connecting to the internet. Currently, wireless connections account for 53% of these internet connections, with this figure predicted to rise up to 67% by 2019.[1] The proliferation of wireless technology has simultaneously improved the potential for people to share their connection with guests or passers by. As of 2017 it is predicted that one-third of consumer owned routers will have the capability to operate a public network of some sort, such as through a separated guest network.[2] This increase in shared internet connections can also be seen on Tor where the number of middle relays within the network has tripled since 2011.[3] When these features are combined, both the growth of connection sharing and also its potential become evident. This growth could be accounted in part to the numerous benefits which have been highlighted in relation to sharing an internet connection through projects such as openwireless.org. These connections not only benefit those seeking to

1 'The Zettabyte Era' – Trends and Analysis, *CISCO*, (June 2015) <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html>

2 M. Jackson, '1 in 3 Routers to Double up as Public Hotspots by 2017', *ISPreview,* (January 2016) http://www.ispreview.co.uk/index.php/2016/01/1-in-3-home-broadband-routers-to-double-as-public-wifi-hotspots-by-2017.html

3 'Tor Metrics – Relays and Bridges in the Network', *Tor* <https://metrics.torproject.org/relayflags.html?start=2011-03-07&end=2016-06-05&flag=Running&flag=Exit&flag=Guard>

access the internet whilst traveling, but can amongst other things help protect privacy and improve the productivity of business.[4] Whilst these factors suggest measures would be promoted to implement safe and user friendly connection sharing, it has largely been ignored in the European legislative agenda. This has created uncertainty from a legal perspective, and vulnerabilities from a technical perspective.

This paper will examine the sharing of residential internet connections, its benefits, potential risks and remedies. Internet connection sharing is the process in which a person facilitates a wireless connection through offering their personal bandwidth. The methods of connection sharing which will be focused on within this paper are through open WiFi hotspots and Tor relays. In the most basic sense a residential WiFi connection is a wireless local area network which allows devices connected to the router to access the internet. These connections are shared when the wireless access is readily available to passers by in some manner. These could be completely open connections such as those which are passwordless and have no registration obligation, or semi-open which include capture pages and a subscription system such as FON.[5] The second form of internet sharing which is being considered in this paper is anonymising services such as Tor. This network functions by connecting users through a series of virtual tunnels rather than making a direct connection, specifically through three different relays.[6] These relays are the servers of volunteer computers who offer to share their internet connection as one of the hops between the users and the website they are trying to connect to. These two examples are not the only types of internet sharing possible in the residential sphere, yet, they are sufficient in typifying the current issues present and can be used to explain how improvements can be made.

The structure of the paper will begin by first clarifying the technology described within this paper, alongside some of the benefits which could be gained from its proliferation. Current case law surrounding this issue – namely *McFadden v. Sony* will also be briefly examined in this section. Secondly, there will be an examination of the current problems facing those who wish to share their residential internet connection. Within this, two major types of risks will be examined: the confusions created by third party traffic; and the potential risk to data through breaches. Following this, possible remedies for the risks highlighted will be suggested both from a legal and technical perspective. These will largely be targeted towards EU legislators, with it being argued that shared internet connections should be a focus within the Digital Single Market initiative(s). Implicitly,

4 https://openwireless.org/

5 FON is a collection of semi-open internet connections around the world. These connections are often in partnership with telecommunications providers such as BT and offer a separate connection from many residential routers. In order to access these people have to be subscribed to the service or pay a fee.

6 'Tor Overview', *Tor* <https://www.torproject.org/about/overview.html.en>

some of these suggestions will also apply to other stakeholders involved in improving the potential of connection sharing such as internet access providers (IAP) and developers of router hard/software. Finally, the problem of liability which could arise from greater connection sharing will be examined. This will be done relatively briefly, with the specific issue of liability a topic which should be examined in greater depth within a follow up paper. Ultimately, it is hoped that this paper will shed some light on the fundamental risks currently present in sharing an internet connection, and offer recommendations for ameliorating these problems.

Background

1. Sharing Benefits

In order to frame why it should be easier to establish shared internet connections it is necessary to mention a few of the benefits. Whilst this is not the purpose of this paper, it would be beneficial to contextualise why it is so important not only to resolve the risks present, but also to promote internet connection sharing for its own worth. These benefits will focus on the quantifiable factors which can be measured from greater access to WiFi, rather than just the mere fact there is a consumer desire for free WiFi – as highlighted in numerous studies.[7] Of the various benefits which could be examined, this section will briefly touch upon three. This is in no means meant to be a comprehensive list of benefits, rather it is meant to concisely frame why reforms could have inherent worth. These benefits will examine the worth shared internet connections can have for individual development, businesses and privacy. Thus, this brief overview of the benefits of shared internet connections seeks to highlight how a number of different stakeholders could benefit from an easier implementation.

The first benefit which could be examined through offering shared internet connection is the empowerment it offers people. This stems from the autonomy it gives individuals in finding information and the greater access it gives people to services. One unique feature of shared internet connections, particularly open WiFi networks is that it offers a public good without discrimination. The European Commission has been taking steps towards creating greater equality on a supranational level through legislating the ceasing of roaming charges as of June 2017.[8] This policy sought to create a level playing field across Europe and prevent discriminatory pricing strategies which could dissuade people from accessing the internet when abroad. Whilst this is beneficial, the

7 S. Taylor et al, 'What Do Consumers Want from Wifi', *CISCO*, (2012), p. 11

8 'Digital Single Market: Roaming', *EU Commission*, (April 2016) https://ec.europa.eu/digital-single-market/en/roaming

ability to access information is still limited to a large extent on price, with phone contracts often offering limited amounts of (expensive) data, and less than 1% of regular WiFi users willing to pay for the connection.[9] As a consequence of this, a proliferation of residential WiFi hotspots would allow those within Europe access to the internet and high broadband speeds without geographical or financial discrimination. The need for internet connection can be seen at an even more fundamental level with many refugees relying on the internet to travel safely from war-torn zones and for contact with their families.[10] This highlights how the benefits range from a vital lifeline for some, to a tool of increasing necessity in the daily life of others. Therefore, shared internet connections could be perceived to lessen discrimination to internet connections, whilst also increasing the ease in which important information can be accessed.

The benefits which could be achieved for business from shared internet connections are also notable. The first example of this could stem from the greater efficiency connection sharing allows for employees. A study by CISCO found that 50% of tablets, laptops and e-reader are connected exclusively through WiFi connections.[11] In parallel to this, 70% of smartphone users regularly supplementing mobile connectivity for WiFi usage.[12] As such, facilitating a greater number of internet connections could allow for work to be done more frequently and effectively when outside of the office. This could empower people to allow them greater choice of when they want to work, and also improve overall levels of productivity within the economy. Similarly, access to the internet allows people to have greater access to e-commerce services or to purchase products online. Having universal instant access to these could be perceived as a factor which stimulates consumer spending due to the greater ease in purchasing created. This factor is evidenced by studies which evidence increasing access to the internet as a key factors in higher levels of consumer spending.[13] Ergo, open internet connections could be perceived as beneficial for business as they could stimulate greater efficiency of staff and also a higher number of sales.

A third benefit which could stem from shared internet connections is the improvements to privacy. This is most clearly shown through the Tor Project where the anonymity of the service is based on volunteers who offer their internet connection as a node.[14] In an age of an increasing number of surveillance measures, anonymising tools could be perceived as an important method for maintaining autonomy.[15] The numerous empowering benefits which could be perceived through

9 Taylor, What Do Consumers Want From WiFi, p. 7
10 A. Ram, 'Smartphones Bring Solace and Aid to Desperate Refugees', *Wired*, (May 2015)
11 Taylor, What Do Consumers Want From WiFi, p. 5
12 S. Taylor et al, What Do Consumers Want From WiFI?, p. 5
13 'Statistics and Market Data about E-Commerce', *Statista* https://www.statista.com/markets/413/e-commerce/
14 'Tor Overview', *Tor* https://www.torproject.org/about/overview
15 For just one example of the pervasive methods see the Investigatory Powers Bill within the UK which allows for

anonymity would be far too broad to cover – so only one example of journalists will be cited here. In the wake of the Snowden revelations many journalists stated how they self-censored or did not investigate topics they were interested in because of the chilling effect.[16] This is damaging for journalists as they are unable to investigate potentially fruitful topics, or issues which might act as necessary scrutiny on the government. Moreover, this feature also damages citizens as it prevents them gaining all the information on the topic which curtails knowledge and can possibly lessen transparency. Considering Tor relies on volunteers sharing their internet connection, a continuation of these is necessary for securing a modern idea of anonymity through tools such as Tor. As such, connection sharing could be seen to align with issues such as privacy, freedom of the press and free speech.

1.2. McFadden Insufficient

There has been a distinct lack of activity in conjunction with the growth of internet connections in the regulatory arena. With this said, one case is currently being heard by the Court of Justice of the European Union (CJEU) in relation to connection sharing. The case of *Tobias McFadden v. Sony Music Entertainment Germany GmbH* is examining the extent to which a person sharing their connection is liable to third party copyright infringements, and whether it is necessary to secure a WiFi network by the means of a password.[17] This case was brought to the CJEU after Sony sought injunctive relief from copyright infringements incurred from McFadden's publicly accessible WiFi network. There has currently been no official ruling on this case which is expected later this year, but the opinion of the Advocate General on the case has been released. This opinion holds that whilst McFadden was not liable for third party traffic on the network, injunctions could be applicable as long as they are not enforced through terminating the internet connection, forced password protections, or through examining all communications transmitted.[18] This ruling would be largely favourable for those wishing to share their internet connection as it affirms that certain features which could have dissuaded those wishing to share their connection are unreasonable.

It is necessary to mention this case here as it has been touted that this ruling will demystify the status of residential internet connections, and thus make the purpose of this paper redundant. Whilst it is true that stating what sort of preemptive injunctions cannot be undertaken will offer greater clarity, it is unlikely to succeed in preventing future litigation. This is due in part to the broad scope

phone-hacking and legs web traffic.

16 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censorship, *Penn America*, (2013), p. 3

17 Opinion of Advocate General Szpunar: Tobias McFadden v. Sony Music Entertainment Germany GmbH (March 2016), Introduction

18 Ibid, Conclusion (4)

it leaves for different types of injunction not specifically mentioned within the McFadden opinion – perpetuating future uncertainty. Similarly, the Advocate General's opinion held the importance of national courts in addressing future cases of injunctions, with it in their jurisdiction to determine a balanced approach in relation to the interests of persons and business.[19] Evident within this is the possibility for future and contradictory precedents being set in different national courts depending on the national emphases in domestic legislation. This can be accounted to the lack of clarity present within EU legislation over connection sharing, a factor which will be covered in greater depth later on in this paper. Moreover, the McFadden ruling would not resolve any of the technical issues which surround connection sharing, many of which could either lead to litigation or the theft of personal data. As such, although a McFadden ruling will certainly help in giving greater clarity to third party liability within Europe, it is restricted in many ways. Consequently, more is necessary, particularly in the legislative sphere to ensure that connection sharing is both safe and clear.

Sharing Risks

One of the serious risks posed by sharing an internet connection is the risk of being held liable for the illicit traffic of others. The risks currently present are unnecessarily high, with various legal and technical opportunities available for minimising these. With this said, the reality of the current framework means that only a select few within Europe have the understanding and technical literacy necessary for safely sharing their internet connection. Similarly, even if all applicable measures are taken to minimise risk, other stakeholders such as law enforcement officials and civil parties could present uncertainty for those sharing their connection. This can be accounted to both a lack of knowledge, and also the lack of clarity currently present with national and supranational legislation. The main risks facing a consumer wishing to share their internet connection will be broken down in to two main issues: the responsibility for third party traffic; and the issues surrounding data protection. The problems surrounding responsibility for third party traffic are largely legal and will include the issues presented by access providers, civil claims and criminal claims. The risks present to data can be accounted to a greater extent as technical issues, with the problems of eavesdropping and access to personal devices issues examined within this paper. In summary, it will be emphasised that sharing of a residential internet connection is currently a complex process which has inherent risks present.

2. Responsibility for Third Party Traffic

19 P. Leersen, Lots to Like in Advocate General's Opinion on Free WiFi and Copyright, *EDRI*, (March 2016) <https://edri.org/lots-to-like-in-advocate-generals-opinion-on-free-wifi-copyright/>

One of the serious risks posed by sharing an internet connection is the risk of third party traffic on a connection. By this it is meant someone who is involved in the traffic, but is not the principal party. In other words, anyone accessing the internet connection who is not under the umbrella category of the home WiFi user. Depending on the set up of the router, this traffic can easily be misconstrued for the traffic of the residents using the router. This is particularly salient if a dichotomy is not made between a private home network and a public guest network. This third party traffic can come as a result of a conscious choice to leave the network connection open to benefit guests and passers-by, or could stem from technical illiteracy. Further, this internet sharing could also come through the establishing of a Tor relay or exit node to facilitate anonymised traffic. A Tor exit node could be misconstrued if the data being sent from Tor is hosted by the same IP address as the home traffic. This section will examine the risks third party traffic presents in different guises, beginning with the failure to uphold a usage policy, followed by civil and criminal complaints.

2.1. IAP Usage Policy

An issue present surrounding liability is the confusion faced by consumers as to whether it is contractually acceptable to host third party traffic on a personal internet connection. The wording of each internet access provider's (IAP's) acceptable usage policy is different, with certain providers not even offering guidance surrounding this issue.[20] This is problematic for a number of reasons. One of the main issues this causes is that users can have their connection shutdown for if sharing is prohibited within the contract. Likewise, even if it is contractually acceptable those wishing to share their connection could be held responsible for third party traffic over their network, leaving scope for the connection getting shut down due to misuse. Again, this puts the pressure on those wishing to provide a public good, with it often a timely process to examine the full acceptable usage policy and/or to contact the IAP for clarity. This point is especially true when it is considered that current legal and technical norms leave numerous other checks necessary for safe implementation.[21] The difficult of this is typified by a German citizen who was inspired to host a Tor exit node and took many of the necessary precautions including checking German law, and also setting up certain host disclaimers. In spite of these precautions, he discovered he was in violation of his virtual service provider's terms of use due to a provision banning the use of anonymous hosting services. As such, if he did not desist from operating his Tor exit node then his contract would have been terminated.[22]

20 When establishing an open connection within the office, our provider Ziggo did not explicitly state within the AUP policy whether hosting third party traffic was acceptable.

21 These include, but are not limited to: establishing a suitable firewall, informing the police and informing the IAP of the desire to host third party traffic. These issues will be touched upon in greater detail later.

22 T. Janik, 'Tor Exit Node for Less Than a Week', *Testbit*, (June 2013) <https://testbit.eu/tor-exit-node-less-week/>

What this emphasises is that there is an inherent difficulty in sharing internet connection, whether this be through a home router or a virtual server. This can be accounted to the vague legal position of connection sharing, and the desire from IAPs to avoid being responsible for any liability. Consequently, the trade off for a user seeking to share their domestic internet connection is significant due to the risk of having the connection terminated, and the time necessary to invest in understanding the acceptable use policy and technical risks.

2.2. Civil Party Claims: Supranational

At both a national and supranational there is inherent legal confusions surrounding the responsibility of passive intermediaries. An examination of legislation and case law surrounding the liability and responsibilities of passive intermediaries best typifies this. In the 2011 CJEU case of Scarlet v. Sabam, a consortium of those interested in protecting against copyright infringements sought to force a filtering system on to a Belgian IAP.[23] This ruling held that according to the *e-Commerce Directive,* an intermediary may not be subjected to using a general monitoring system.[24] This ruling further stated that such a system is not a fair balance between copyright, privacy and business, as it "would require that ISP to install a complicated, costly, permanent computer system at its own expense" which also infringe users' privacy.[25] A separate 2014 case of *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH* ruled that the IAP in question, UPC, had a duty to block users' access to copyright infringing websites.[26] The judge ruling on this case stated: "It must be held that an internet service provider, such as that at issue in the main proceedings, which allows its customers to access protected subject-matter made available to the public on the internet by a third party is an intermediary whose services are used to infringe a copyright or related right within the meaning of Article 8(3) of Directive 2001/29."[27] This ruling was based on the Copyright Directive, with Article 8(3) stating that "member States shall ensure that rightsholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right."[28] The implication of this is that even passive intermediaries such as IAPs are burdened with the duty to prevent copyright through blocking users' access to certain websites. Whilst both these cases can be reconciled by the fact that the UPC ruling does not

23 'Summaries of Important Judgments', *EU Commission* <http://ec.europa.eu/dgs/legal_service/arrets/10c070_en.pdf> (May 2012)
24 Schellekens, 'The Internet Access Provider: Unwilling or Unable', *International Journal of Law and Information Technology,* p. 314-315
25 Ibid, p. 315
26 'Judgement of the Court: UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH', *Curia,* (March 2014) <http://curia.europa.eu/juris/liste.jsf?language=en&td=ALL&num=C-314/12>
27 Schellekens, The Internet Access Provider, p. 312
28 Directive 2001/29/EC

demand a monitoring system explicitly, it has widely been noted that such a monitoring system would be the only way to enact the ruling.[29] As is clear from these cases, decisions surrounding passive intermediaries based on European law often prove unpredictable as no clear precedent within the area has been set as to what duty passive intermediaries have. Although these two examples have focused to a greater extent on IAPs, many of the rulings could be perceived to apply to those wishing to share their internet connections. This uncertainty highlights the difficulty those wishing to share their residential WiFi face from third party copyright infringements due to the lack of clarity present at a supranational level.

2.3. Civil Party Claims: National

At a national level, the approaches and implementations of the *2001 Copyright Directive* and *2000 e-Commerce Directive* can be seen to differ. This is not only due to the axiomatic nature of a European directive to be interpreted by national legislatures, but also because of their lack of precision surrounding WiFi as a technology, which was at its commercial inception during this period. Until a recent amendment to the *Tele Media Act,* Germany had a particularly negative approach to connection sharing. This approach (known as the norm of S*törerhaftung)* was developed through analogy in case law and held that password protections were necessary for WiFi connections in order to dissuade third party copyright infringements.[30] This approach placed part of the liability on those passive intermediaries who shared their network connection through a fine system based on preventative injunctions.[31] A similar (albeit less draconian) approach was employed in the UK where IAPs were required to prevent third party infringements as long as they were not too 'burdensome'.[32] This 'moral duty' is enforced by the British telecommunications regulator OFCOM who provide a three-strike rule in terms of preventing copyright infringements before prosecution is considered.[33] This amongst other regulatory features implies that the British approach promotes IAPs recording users' personal data, download history and file sharing in order to facilitate prosecution. Although this rule has generally been applied to IAPs as opposed to those sharing their internet connection, it is not hard to see how measures such as a monitoring burden implied in the *2010 Digital Economy Act* could also be translated into a domestic domain. These heavy-handed approaches highlight how certain interpretations of EU law have given a greater

29 Schellekens, The Internet Access Provider, p. 310
30 C. Busch, Secondary Liability for Open Wireless Networks in Germany: Balancing Regulation and Innovation in the Digital Economy, *SSRN,* (2015), p. 3
31 K. Grieshaber, 'German Court Orders Wireless Passwords for All', *NBC News, (*December 2010) http://www.nbcnews.com/id/37107291/ns/technology_and_science-security/
32 L'Oreal SA & Ors v EBay International AG & Ors, (2009), 456-464
33 B. Collins, 'Ofcome Warns off Free WiFi Providers', *Alphr,* (2010) http://www.alphr.com/news/security/358342/ofcom-warns-off-free-wi-fi-providers

focus on copyright legislation, resulting in both liability and burdens for passive intermediaries.

Alternative approaches have been taken elsewhere within Europe, with greater emphasis being placed on Article 15(1) of the *e-Commerce Directive* which prohibits the obligation to monitor traffic.[34] The Dutch *Burgerlijk Wetboek* (civil code) sees no general obligation to monitor the information which the providers transmit or store, as long as they are only 'transmitting' and 'providing access' to data and the internet (a mere-conduit).[35] In spite of this legislation, Dutch courts have held that sometimes exceptions need to be read in when it comes to copyright infringements. In the case of *BREIN v. KPN Telecom B.V.* the defendant was an IAP performing mere-conduit activities through facilitating the traffic of a torrenting website. The court ruled that the IAP was required to shut down the internet connection of the subscriber running the illicit website if they were to re-open the website or another with a similar purpose.[36] This highlights how although IAPs are not obliged to monitor, they can on occasion get ordered to block infringing users. Moreover, *the Gedragscode Notice-and-Take-Down* (Notice and Take down Code of Conduct) provides standard procedures for intermediaries who provide a “public telecommunications service on the internet” for whether to remove unwanted content.[37] Although this is not a statutory law, many IAPs have enforced these policies, with considerations of 'undesirable' largely based on consumer agreements.[38]

The liability and burden bearing within the Netherlands can thus be contrasted with that of the UK. The burden of discovering illicit content is placed solely on copyright holders, with the Dutch IAPs taking requests and choosing to shut down or not in accordance to this. This prohibition largely shifts the enforcement burden away from the IAPs and enforces their position as passive intermediaries as stated in the *e-Commerce Directive*. In terms of residential connections this is beneficial as it implies that the burden (if any at all) placed on those sharing their internet connection would be minimal if given the same status as IAPs. This is because of both the relatively minor burden placed on passive intermediaries, and also current technical limitations on commercial routers for blocking users. The contrast between the Netherlands, the UK, and Germany highlights the inconsistencies present with copyright enforcement and how burden and liability differ in respective countries.

2.4. Criminal Risks

34 Directive 2000/31/EC, Article 15(1)
35 N. van Eijk et al, 'Moving Towards Balance: A Study Into Duties of Care on the Internet', *IViR* (2010), p.50
36 Ibid, p. 64
37 Ibid, p. 52
38 Ibid, p. 52

Arguably the most personally damaging consequence of sharing an internet connection comes from law enforcement agencies such as the police. Stories of police confusion leading to early morning raids due to shared connections have been noted in news article and blog posts.[39] Although not widespread, this has proved an issue for those sharing their internet through a Tor exit node where it can appear that illicit information is being accessed or shared from the exit node's IP address. It is particularly problematic on Tor because of the anonymity of the service, and also because it can sometimes facilitate access to illicit onion services. It is this negative portrayal Tor as well as a lack of technical understanding from law enforcement agencies, which can create the risk of having computer servers seized and analysed by the police – as has been reported across Europe.[40] More serious cases of punishment have been noted, such as for an Austrian hosting a Tor exit node who was found guilty of ferrying child porn, and in turn given three years probation and fined €30,000 .[41] It was widely commented that if he had challenged the ruling in a higher court then it would have likely been overturned, however, economic constraints prevented this. These instances exemplify how the lack of clarity surrounding Tor exit nodes creates criminal risk from third party traffic. It is necessary to point out that legal challenges are not just limited to Tor exit nodes, and have also been applicable to other forms of connection sharing. One example of this is in Scotland where a residential home WiFi router was not password-protected, resulting in a passer-by downloading child pornography.[42] In this case the man subsequently found himself under suspicion of accessing the content as it was his connection that was used. It is evident from these examples how third party access can create issues due to the illicit traffic from a guest being misconstrued for that of the primary-user's.

3. Risks to Data:

A second set of risks which are present when sharing a residential internet connection is the risks to personal data of those sharing their internet connection. If certain security precautions are not in place then the radio signals sending the data from the home devices to the router can be

39 M. Kaste, 'When a Dark Web Volunteer Gets Raided by the Police', *NPR*, (April 2016) <http://www.npr.org/sections/alltechconsidered/2016/04/04/472992023/when-a-dark-web-volunteer-gets-raided-by-the-police>

40 J. Cox, 'The People who Risk Jail to Maintain the Tor Network', Motherboard, *Vice* (April 2015) <https://motherboard.vice.com/read/the-operators>

41 D. Pauli, 'Austrian Tor Exit Relay Operator Guilty of Ferrying Child Porn', *The Register*, (July 2014) <http://www.theregister.co.uk/2014/07/04/austrian_tor_exit_relay_op_found_guitly_for_ferrying_child_p0rn/>

42 T. Porter, 'Paedophiles and Criminals Using Open WiFi Networks, Warn Police', *International Business Times*, (February 2014) <http://www.ibtimes.co.uk/paedophiles-criminals-using-open-wi-fi-networks-warn-police-1434820>

compromised. These risks to data are damaging because of the threat they present to privacy, with many personal documents facing the possibility of being snooped on. Moreover, data leaks could prove dangerous due to the risks present in terms of fraud or cybercrime from information such as passwords or banking details being accessed. The risks to personal data will be examined in two main sub-categories which are eavesdropping and access to home devices. These topics will seek to emphasise how there are numerous risks present to data when sharing an internet connection if security measures are not implemented.

3.1. Eavesdropping

A major concern from the perspective of sharing an internet connection is the potential for eavesdropping on open internet connections. Eavesdropping encompasses a number of different methods employed by hackers, but in essence involves intercepting data in some way in-between the device and access point. A few different types of eavesdropping will be cited within this section to highlight how the methods range from amateur attacks, to complex encryption stripping tactics can compromise personal data. The first type of attack that can take place is session hijacking attack which can be undertaken through simple tools such as *Cookie Cadger* (or the more well known, but now discontinued *Firesheep*).[43] These simplistic tools capture the cookies which contain log in details for a specific website, and from this the hacker is able to do everything the user can do on an unencrypted website.[44] This means that private data such as messages could be read and also altered by those accessing the session. Similar threats to data are present through man in the middle attacks (MITM). This attack does exactly what the name implies and intercepts data through placing itself in between the user and either the router or the server hosting the webpage. One version of this attack is packet sniffing traffic, an attack which examines unencrypted data through reading the plain text. This attack is relatively simplistic, with publicly available software and easy to use software enabling this.[45] The ease in which this can be done is evidenced by the readily available application 'Fing', available for phones using Android or iOS operating systems, which allows users to intercept traffic traveling to the access point.[46] Through data interceptions such as this, unencrypted sensitive data ranging from the content of messages to credit card details can be picked up by hackers. A more complex version of this attack is an ARP spoofing attack in which an attack changes the flow of traffic, and is thus able to read, insert, and modify messages between two

43 For more information about Firesheep see <http://codebutler.com/firesheep/>
44 E. Butler, 'Firesheep', *Codebutler,* (October 2010), <http://codebutler.com/firesheep/>
45 T. Mirzoev & S. White, The Role of Client Isolation in Protecting WiFi Users from ARP Spoofing Attack, *I-managers Journal on Information Technology* (2014), p. 12
46 'Tainted Love: How WiFi Betrays Us', *F-Secure* (2014), p. 20

communication parties.[47] In this sense it is similar to packet sniffing, but the user is able to access encrypted data, meaning areas which were perceived as secure such as banking websites are liable to attack.[48] All these types of eavesdropping can target a person sharing their home internet connection for if they have not separated their traffic. This highlights how the data of those sharing their internet connection is often liable to amateur hacks such as packet sniffing, and also more complex attacks which can circumvent HTTPs encryption.

3.2. Access to Personal Devices

A second concern surrounding data when sharing internet connection is the possibilities surrounding access to personal devices and files. Generally speaking domestic local networks tend to have lower security levels as they trust the other devices on the network. The problem comes when higher levels of security are disabled when the residential connection is being shared. Applications such as *Who is on My WiFi* can be downloaded and used to examine who else is accessing a certain WiFi connection. This is problematic as personal information about a device, such as its MAC address, IP address and perhaps computer name. Alongside this, when on a home network the firewalls and other defences are often less secure, or not implemented on devices. This can be shown through one of Windows' features which seeks to protect against unwanted file sharing. When connecting to a new WiFi hotspot, a pop-up appears asking what type of location the computer is connecting to (i.e. home, work, or public).[49] This simplified interface is a safety precaution taken by Windows in an attempt to protect documents through automatically disabling file sharing, network discovery and public folder sharing.[50] In spite of this precaution, when connecting to a home WiFi connection it could be tempting to set the firewall settings accordingly without realising the damage others connecting to the network could cause. What this seeks to highlight is how when sharing a network connection it is relatively easy to leave devices both detectable and unprotected against attacks from those with malicious intent.

Without firewalls and other protections present on devices, a computer could be liable to a number of different attacks. One example of this is when firewalls do no prevent file sharing; if connected to a hub based WiFi connection, then any other person on said network would be able to access shared files.[51] The problem with this is evident for if any personal, or work related files are set to

47 Mirzoev, The Role of Client Isolation in Protecting WiFi Users, p. 12
48 Ibid, p. 13
49 C. Hoffman, 'HTG Explains: Why you Shouldn't Host an Open WiFi Network', *How to Geek*, (August 2013) <http://www.howtogeek.com/132925/htg-explains-why-you-shouldnt-host-an-open-wi-fi-network/>
50 B. Burgess, 'Keep Your Windows Coputer Secure on Public Wireless Hotspots, *How to Geek*, (August 2010) <http://www.howtogeek.com/howto/26674/keep-your-windows-computer-secure-on-public-wireless-hotspots/>
51 K. Lawson, 'Are Your Shared Files at Risk on a Hotel Network?', *Private WiFi* (Novermber 2011)

shared which a person does not want stranger to know about. This could compromise a user on a number of different levels, but most obvious is the potential is the theft of personal information which could lead to identity theft. Arguably more damaging than this is the possibility for malware to be planted on to any computer sharing the connection. Malware's purpose is to perform unwanted tasks on the infected computer, usually to benefit some third party, with the negative benefits ranging from pop-ups to stealing passwords.[52] What's more, malware has an ability to infect other devices which are connected to a local network, meaning that all home devices could in turn be compromised without a user realising. Therefore, sharing a network without applying adequate protections can leave devices visible and accessible for others to take personal documents, and also to act as a bot for their actions.

Suggestions for Safer Internet Sharing:

The Digital Single Market is a set of initiatives which seek to extend the single market to the digital realm through a harmonisation of national policies. It can be defined as "[a market] in which the free movement of persons, services and capital is ensured and where the individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence."[53] The important aspect in relation to the sharing of connections is the focus on access to the internet, which is the first of three-pillars stated in the initiative. To some extent this has been addressed by the EU policy of annulling roaming charges in order to ensure connectivity across Europe.[54] In spite of this progress, it could be perceived as unsustainable, with a 2013 study by the European Commission emphasising the necessity of investing in more WiFi to off-load some of the burden from the already congested 3/4g networks.[55] Similarly, another focus within the Digital Single Market initiatives is the push to "safeguard an online environment through providing the highest possible security and freedom for everyone."[56] Both the desire for greater access to the internet and also the push for greater security mirror the aims of increasing the number, and improving the quality of shared internet connections. Ergo, this section of the paper will seek to offer suggestions for how safer internet connections can be implemented, and how these policies fit

<http://blog.privatewifi.com/are-your-shared-files-compromised-on-a-hotel-wifi-network/>

52 'Viruses, Spyware and Malware', *Information Systems and Technology,* <https://ist.mit.edu/security/malware>

53 'Digital Single Market: The Strategy', *EU Commission,* (February 2016) <https://ec.europa.eu/digital-single-market/digital-single-market>

54 'Digital Single Market: Roaming', *EU Commission,* (April 2016) <https://ec.europa.eu/digital-single-market/en/roaming>

55 'Europe Loves WiFi: New Study Recommends More Spectrum Should be Available', *European Commission,* (August 2013) <http://europa.eu/rapid/press-release_IP-13-759_en.htm>

56 Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace, *EU Commission,* (February 2013), p. 4

within the scope of the Digital Single Market.

As is apparent from the focus on the Digital Single Market, the suggestions will be largely targeted at legislators. With this said, the Cybersecurity Initiative highlights the necessity of the various different stakeholders working in tandem in order to achieve the best results in alleviating the problems.[57] As a result, many of the suggestions forwarded in relation to the Digital Single Market will also implicitly, or explicitly apply to other stakeholders such as IAPs, router developers and also those sharing their connection. Within this, two main trails of argumentation will be followed. Firstly, it will be propounded that greater legal clarity and lesser contradiction between current legislation would mitigate the risks of prosecution and inconsistency. This point is particularly true of copyright legislation and enforcement which often proves contradictory and is a serious barrier to harmonisation. Secondly, it will be argued that a policy of security by design through increasing the required technical defences would significantly improve the cybersecurity of both those offering and accessing shared internet. It is necessary to emphasise the importance of these recommendations being read in conjunction, with neither a technical, nor legal approach offering a sufficient outcome alone. Whilst it is accepted that the proposals of this paper will not provide a fully secure method for sharing an internet connection, their adoption would signal a marked improvement on the current implementation.

4. Legal Clarity

4.1. Digital Single Market:

An issue with the McFadden opinion is that it would not resolve some of the inherent contradictions in EU law. This means that although the precedent set may hold some worth, it is likely that lawmakers may transpose legislation unwittingly, leading to future cases of litigation. For example, the McFadden opinion still allows for injunctions as long as they are not based on failure to terminate the connection, enforce password protections, or monitor the connection.[58] The different focuses within national law, combined with the extensive scope for interpreting preventative injunction provides the possibility (if not probability) of future litigation. An example of this is the recently revised German *Tele Media Act* which states that 'appropriate security measures against unauthorized access are necessary.' This language typifies how those who are unhappy with infringements such as copyright holders could still seek preventative injunctions based on more niche aspects such as the technically capacity of a router to filter. These issues are also present for

57 Ibid, p. 4
58 Opinion on McFadden v. Sony, Conclusion (4)

Tor, with scope left within this ruling for preventative injunctions to be made against those operating exit nodes and not closing certain ports. This point is particularly true because of the linguistic focus on economic activity present within the McFadden opinion, which could lead to future challenges of non-commercial enterprises. Litigation stemming from vague rulings can be seen from the previously mentioned case of *UPC v. GmbH* where an injunction to block access to webpages was demanded, in spite of the previous *Scarlet v. SABAM* case prohibiting monitoring obligations. Although broad injunctions such as these are not valid, it emphasises the likelihood of further challenges to seemingly clear provisions.[59] Therefore, it could be suggested that legislation of some sort alongside a McFadden ruling could help for a coherent, Europe-wide level of clarity surrounding issues of internet sharing.

One possible method for circumventing future litigation is through a revision of the current categories stated in the *e-Commerce Directive.* The Commission *has* stated that it seeks to clarify intermediary liability, yet, has said that the categories established in the *e-Commerce Directive* are sufficient.[60] In parallel to this, the initial statements emerging from the Commission imply that voluntary actions by IAPs will be a large part of the resolution for copyright infringements.[61] These features imply that the focus of any reforms which take place will focus on IAPs and online service providers such as Facebook. What this suggests is that little thought or attention has been paid to the role of passive intermediaries who wish to share their connection in the residential sphere. The Digital Single Market initiative offers the perfect opportunity for clarity to be provided for those wishing to share their internet connection through codifying specific provision directly relating to WiFi and Tor connections in relation to the mere-conduit clause of the *e-Commerce Directive.* This could be done through offering a closer reading of the mere-conduit clause to affirm that non-commercial sharing which does not collect data undoubtedly counts as a passive intermediary. Doing this would be in line with the Commission's aim of enforcing comparable rules for comparable digital services – in essence giving those sharing their connection the same liability as telecommunications providers for unfavourable content.[62] By this it is meant that mere-conduits should not face liability, but can take voluntary steps for alleviating copyright abuses or illicit content. Although this currently seems evident within the language of the clause, the continued lengthy seizure of servers and fine the Austrian who ran the exit node highlights the current uncertainty. As such, this reading would allow for a modernisation of understanding on issues such

59 Ibid, section 108-110
60 N. Rose & B. Potts, 'Leaked Commission Communication – No Change for Intermediary Liability Regime', *Lexology*, (May 2016) <http://www.lexology.com/library/detail.aspx?g=4f7749dc-a1b6-4814-9aa6-6e2385e0ce85>
61 'Commission Updates EU Audiovisual Rules and Presents Targeted Approach to Online Platforms', *EU Commission*, (May 2016) <http://europa.eu/rapid/press-release_IP-16-1873_en.htm>
62 Ibid

as copyright and the tacit trafficking of illicit content. A clause explicitly specifying the reach of mere-conduits in relation to residential internet connection could therefore be beneficial in preventing an excessive burden being placed.

4.2. Good Samaritan Clause

A further measure which could be implemented within the proposed modernisation of legislation across Europe is a Good Samaritan Clause. As highlighted earlier in this paper third party liability is a confused issue across Europe, with it questionable as to whether a McFadden ruling would fully resolve these issues. In 2009 the case of *BREIN v. Mininova* the judge ruled that Mininova (a torrenting website) was liable for copyright infringing material on their website as they had the ability to filter content, but chose not to for copyrighted material.[63] Implicit within this ruling was a choice for intermediaries to either filter entirely, or not employ any method whatsoever. If a ruling such as this was to be made in the realm of residential connection sharing, then it could prove a significant factor in dissuading people. This is because it creates uncertainty over the implementation of voluntary measures to prevent unwanted material or copyright infringements. For example, Mininova filtered content such as pornography and viruses from user's results, a feature which would benefit users through offering them greater protections and a better service.[64] The *BREIN v. Mininova* case dissuades intermediaries from offering any sort of protections for those accessing their service as it creates uncertainty and potential liability issues. This could be translated to both open WiFi connections and also Tor. Those offering to share their WiFi may be unwilling to partake in URL filtering or the limiting of bandwidth, as by placing the effort in they may be demanded to do more. Technical features such as the blocking of certain ports on an exit node could also be considered to come under this umbrella. Damage from this could both offer weaker protections for those accessing the shared connection, but could also lessen the overall safeguards against the accessing of unfavourable content. The uncertainty a ruling such as this would present, or even the possibility of a ruling such as this taking place could weaken current protections in place. Consequently, legislation against arbitrary rulings such as this is necessary in order to maintain high levels of voluntary protections for both the users, and also other interests such as copyright holders.

The Good Samaritan Clause present within the Communications Decency Act of the U.S. states that “no provider or user of an interactive computer service shall be treated as the publisher or speaker

63 Van der Sloot, 'Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law,* (2015), p. 214

64 Ibid, p. 214

of any information provided by another information content provider."[65] Further, no provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers objectionable.[66] This sort of legislation could clarify liability for those wishing to share their internet connection and prevent preemptive injunctions based on not implementing certain features for some content. Through featuring a Good Samaritan clause, user liability and protections would become far clearer due to the fact they could not get penalised for voluntary measures. This would not only encourage those who are sharing to improve their own security, but would also promote measures against copyright infringements (as could be seen by voluntary measures taken by U.S. ISPs.) As such, the greater clarity provided by a Good Samaritan Clause could benefit society through more readily available WiFi, whilst also protecting copyrighted material and preventing unnecessary legal cases.

4.3. Clear Acceptable Usage Policy

In the short term, greater clarity of the mere-conduit clause and a legal codification of its applicability to those sharing their internet connection could create more work for IAPs. This is because a greater number of complaints could be presented due to an uptake in the number of people sharing their internet connection. In spite of this, in the longer term if technical measures were established to provide greater clarity over which connection is shared, the overall work could decrease.[67] This is because more shared internet connections would demand a more effective way to distinguish between private and public, leading to an easier recognition than is currently present. Similarly, this greater legal clarity could prove beneficial as it could further affirm the liability people face, whilst also sharing the voluntary burden of preventing malicious traffic. In order for these factors to be achieved the IAP acceptable use policy has to make clear that connection sharing is acceptable and that there are mere-conduit protections within Digital Single Market legislation. This could be implemented through a legislative approach, or more beneficially from internal policy. If legislation is clear surrounding liability and there is an effective system in place highlighting which routers are open (a point which will be covered later), then there is little reason why an IAP should want to prevent connection sharing. If anything, the opposite is true – offering connection sharing as a default creates a better product, in theory making the IAP more attractive. If a norm of greater clarity was present then this would be beneficial for those wishing to share their connection as the risk of having the connection shut down for third party abuse is minimised.

65 '47 U.S. Code Section 230 - Protection for Private Blocking and Screening of Offensive Material', *Cornell University Law School,* <https://www.law.cornell.edu/uscode/text/47/230>

66 Ibid

67 Greater clarity of these technical points will be offered later within this paper.

Consequently, if greater legal clarity was present then clear acceptable use policies which allow for connection sharing would benefit both IAPs and users of the service.

5. Technical Suggestions

The Digital Single Market also forwards the necessity of creating the right conditions for digital networks and services to flourish. Within these initiatives is also a cybersecurity strategy which seeks to create an 'open, safe and secure cyberspace' in the face of increasing cyber-attacks. This strategy has led to broad stroke measures in an attempt to protect citizens, including the creation of a European Cybercrime Centre, and legislation offering harsher penalties to hackers.[68] Whilst these measures are beneficial, significant amounts of cybercrime could be prevented through more basic policies aimed at a user level. Promoting an approach of secure by design at a consumer level could protect both those wishing to share their connection, and people who access public WiFi hotspots. The self-explanatory of secure by design holds that software should be built from the ground up in order to be protected from malicious attacks. This policy is already heavily implied in terms of connection sharing within EU legislation through Article 4 of the Directive on *Privacy and Electronic Communications (2002).* This article holds that "providers of publicly available electronic communication services (which include Internet service providers as well) are required to take appropriate technical and organizational measures to safeguard the security of the services provided. The measures to be taken should ensure a security level that is proportionate to the state of the technology and the costs of its execution."[69] Due to the constraints of current consumer technology, as well as the encryption of websites themselves, it is near impossible for those wishing to share their internet connection to put in place viable protections for the data of those accessing the connection. This could suggest that more specific regulations surrounding router specifications could be necessary, or an independent promotion by other stakeholders to improve technological standards. This section of the paper will emphasise measures which could be implemented which adequately protect user data on the one hand, and allowing business the freedom to conduct their activities, and not placing unreasonable burdens on consumers on the other.

5.1. The Futility of Password Protections

A suggested solution for the issues presented by sharing internet connection has been to enforce password protections on to routers. Policies such as this one seek to hinder the access of those with

68 'Commission to Boost Europe's Defences Against Cyber-Attacks, European Commission (September 2010), <http://europa.eu/rapid/press-release_IP-10-1239_en.htm?locale=fr>

69 van Eijk, Moving Towards Balance, p. 12

malicious intent, whilst also making wrongdoers more identifiable. Although this strategy has some worth for protecting those who wish to keep their network private, it does not resolve the fundamental issues present with network sharing. This point could be seen in practice by the German retraction of forced password protections which proved to be a failed experiment. It has been noted that enforced password protections, or the forced disclosure of personal information dissuades users from accessing said hotspots which undermines the benefits for consumers and business.[70] Both studies and practices have emphasised the demand and usefulness of open internet points, with the Freifunk movement one of many responses to forced password protection policy. This movement promotes free internet access, and in response to the German S*törerhaftung* norm Freifunk attained their internet from a Swedish IAP via an anonymised VPN.[71] Even more fundamental than the consumer demand is the fact that numerous security issues highlighted are also present within password-protected hotspots. If the data being sent is unencrypted, then those with access to the password on a protected network are still able to perform packet sniffing and session hijacking. Similarly, the same risks surrounding a MITM attack are present, even if the traffic is encrypted through HTTPs.[72] It is necessary to note that certain certification-based systems such a the Eduroam model used for universities could overcome many of these security issues, yet, would likely be inviable on a mass-consumer level and would also not be truly open and private.[73] Thus, a policy of password-protection would not only be counter-intuitive to the consumer demand for readily available WiFi, but would also not resolve many of the security issues.

5.2. HTTPs Encryption

In Article 16(1) of the *Treaty of the Functioning of the European Union* it states that every person has the right to the protection of personal data concerning him or her.[74] Similarly, the *General Data Protection Regulation* (GDPR) states that "the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the regulation."[75] What these clauses imply is that if personal data is being transmitted then extensive protections should be put in place in order to ensure that the data is protected to the maximum extent. One of the most applicable ways of forwarding this in practice is through the promotion of HTTPs encryption. In essence, this is a HTTP form of data transferring, however, it contains SSL or TLS meaning only the user's computer and the secure server can

70 Opinion on McFadden v. Sony, 138-139
71 J. Lenhardt, 'Friefunk Statt Angst', (July 2012), <http://writing.jan.io/2012/07/26/freifunk-statt-angst.html>
72 'Understanding the WPA2 'Hole 196' Attack: Vulnerabilities & Motorola WLAN Countermeasures', *Motorola* (2010) <http://www.airdefense.net/whitepapers/UnderstandingWPAWPA2Hole196Attack_TB_0810_chv4.pdf>
73 For more information see <https://www.eduroam.org/eduroam-security/>
74 Treaty of the Functioning of the European Union, Article 16(1)
75 Regulation 2016/679/EC, Article 24(1)

recognise the data. HTTPs has been adopted and promoted in areas ranging from major ISPs such as Facebook and Google, to the U.S. Federal Government.[76] Although from a technical perspective HTTPs encryption is far from perfect, and is still liable to certain types of man in the middle attacks, as a whole it can prevent amateur session hijacking using tools such as Firesheep.[77] Further, HTTPs encryption could also help prevent packet sniffing at a Tor exit node which could give personal data away about a person. This means that a promotion of HTTPs encryption would also help improve anonymity on Tor. As such, one recommendation could be the official promotion of, or legislating surrounding requirements for website encryption. This could be implemented in different ways, including a pop up warning (similarly to the cookies acceptance pop up) that a connection is not secure. A more effective strategy could be to legislate HTTPs by default. This could prove more problematic due to factors such as the inability of older software to support newer methods of encryption, nonetheless, would be worth the trade-off in the longer term.[78] Therefore on method of empowering users and strengthening data protection could be the greater promotion of stronger levels of traffic encryption such as HTTPs.

5.3. Router Default Split

A further option available for improving internet sharing includes the development of a better standard of router. In order to do this, both IAPs and developers would have to work in tangent. Increasingly, IAPs are offering 'public' hotspots to those who are subscribed to their network, through offering a separate connection, with BT in the UK having over 5 million of such connections.[79] Whilst in principle this sounds beneficial, it can in fact have dis-empowering effects, whilst also damaging market competition. A 2012 study by Cisco examining user tendencies and WiFi found that 50% of participants were likely to switch to an alternative telecommunications provider if free WiFi at numerous points was provided.[80] The importance of WiFi access to consumers not only affirms the importance of open WiFi, but also highlights the monopolising effects which could be had upon a market. With only a handful of telecommunications providers currently used widely within the market, there is a difficulty for new companies who wish to enter the market to able to offer widespread access to WiFi points. This is because they cannot utilise a base of customers' routers to double them up as public hotspots. This is damaging as it further prevents competition in a market already dominated by a handful of companies. Similarly, many

76 T. Scott, 'Policy to Require Secure Connections Across Federal Websites and Web Services', *Executive Order of the President*, (June 2015) <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf>
77 Mirzoev, 'The Role of Client Isolation in Protecting WiFi Users', p. 12
78 Z. Zorz, 'Google Starts Tracking, Encourages Worldwide HTTPS Usage', *Helpline Security,* (March 2016) <https://www.helpnetsecurity.com/2016/03/16/worldwide-https-usage/>
79 'About BT WiFI, *BT,* <https://www.btwifi.co.uk/>
80 Taylor, 'What Do Consumers Want From WiFi, p. 8

users are unaware or unable to change the fact that their internet connection is being shared by other subscribers.[81] This feature of fractious sharing disempowers users from making a choice about how, and who they want to share their connection with. These factors imply that in order to best empower consumers and stimulate competition IAPs should offer a separate guest network which the consumer has a choice over.

In order to ensure that those wishing to share their internet connection are empowered, better hard/software needs to be produced by the developers. One key feature surrounding this is providing commercial routers with a default split between a private internet connection and a guest network. To some extent, this change could already be seen to be taking place, with it being predicted that by 2017 the hotspots in one-third of houses will also have a public WiFi connection of some sort.[82] Further promoting this software by default would help limit the extent to which third party traffic could be deemed to be coming from the resident offering the shared connection. This is because there would be an exact dichotomy between home traffic, and the traffic of those accessing the open hotspot, creating greater clarity for if the open connection was to be misused and needed to be investigated. Currently in a number of routers this feature is obscure within the set up, with many others not possessing it, meaning that software such as OpenWRT needs to be installed.[83] These features are inaccessible to many users because of a lack of technical knowledge. When a split by default is combined with the greater legal clarity provided by legislation and a clear McFadden ruling, legal confusion surrounding liability for malicious traffic on a network is likely to be alleviated to a large extent. In principle, this split could benefit those wishing to share their connection through offering a Tor exit node also. This is because it is less likely that traffic will be mistaken as there is an exact split between the connections being offered. Thus, better technology would not only empower users, but will also demystify legal wrongdoing for law enforcement officials.

5.4. Reverse DNS

In order to maximise the success of offering easier shared networks, it would also be advisable to include features to make IAPs and others who view the network aware that the traffic is stemming from a shared network. Many of these suggestions are already listen on the Tor website for those running an exit node which aim at increasing the transparency over the purpose of the connection.[84]

---

81 M. Jackson, '1 in 3 Home Boradband Routers to Double as Public WiFi Hotspots by 2017', *ISPreview,* (January 2016) <http://www.ispreview.co.uk/index.php/2016/01/1-in-3-home-broadband-routers-to-double-as-public-wifi-hotspots-by-2017.html>

82 Ibid

83 'Routers', *Open Wireless Movement,* <https://openwireless.org/routers>

84 Legal FAQ, *Tor, (*April 2014) <https://www.torproject.org/eff/tor-legal-faq.html.en>

Firstly, it would be beneficial to establish a reverse DNS name for the IP address to make it clear that the traffic stemming from the network can be accounted to third parties. Similarly, it is suggested that when running a Tor exit relay that a disclaimer is established to explain Tor, legal aspects surrounding it and that logs of traffic are not kept. The same principle can be applied to shared wireless connections. Whilst they suggestions could be considered to be largely targeted at the people wishing to share their internet connection, some of these could be considered as features which could be included in the set up of a guest network on a router. Alongside this, IAPs could consider splitting the set IP addresses between those which are used for private and public connections, with the latter searchable through an organisation such as Ripe NCC. The inclusion of features such as these could help prevent unnecessary confusion creating greater ease for both those wishing to share their internet connection, and those seeking to prohibit illicit content.

5.5. Router Controls

As well as helping protect against liability issues for connection sharing, the implementation of a Good Samaritan Clause could play a key role in the promotion of better router technology. The policy reasoning behind the Good Samaritan Clause in the U.S. states that it was implemented for the promotion of a competitive free market unfettered by Federal or State regulations, the encouragement of the development of technologies which maximise user control, and to remove disincentives for filtering.[85] Each of these benefits could be seen as applicable to the EU. A Good Samaritan Clause could promote the development of more secure router software and better filtering systems through stimulating competition to produce such routers. Through this, many features present on enterprise standard routers could be translated down to commercial routers, and in turn empower those wishing to share their internet connection. These greater levels of empowerment would give users the option to implement some of the suggestions forwarded, whilst leaving them to face no repercussions for not implementing them, or not implementing more.

A few of the possible filtering systems which could be implemented will be forwarded within this section. These features could be featured clearly within the set-up, or within an easy to use interface – however, the specifics of possible implementations will not be covered here. A feature which could prove highly beneficial would be the ability to detect infected computers when they attempt to connect to the hotspot. This could prove successful in preventing bots connecting to the network which could infect other computer or send out spam. A further possibility which could be included is the ability to adjust and limit the bandwidth, upload and download speeds on a guest network. This could benefit those sharing their connection as they could choose to set the bandwidth to levels

85 B. van der Sloot, Welcome to the Jungle, p. 215

which they are willing to share on their network. This could both prevent the uploading of illicit content, and also prevent one user from consuming all the bandwidth. Similar benefits could be gained from features such as URL filtering which would make it more difficult for those accessing the network to connect to sites which facilitate illicit material. Again, the decision to filter would be left up to those sharing their internet connection, as well as the choice to filter what they perceive as undesirable. A final feature to be mentioned is the storage of the IP and MAC addresses of those who connect to the guest network. Information such as this could be useful in blocking access for those who misuse the connection. Whilst this could be useful, it also comes with legal risks as a MAC address combined with geo-location means that data could be considered personal and has to be protected accordingly.[86] As such, for storing data such as this it would be necessary to have a Good Samaritan Clause in place, and also strong router encryption to ensure that there are no data breaches. Consequently, a Good Samaritan Clause could prove beneficial in digitising the European economy through the promotion of better technology standards and empowerment of people.

A further suggestion which could benefit the security of those seeking to share their internet connection is client isolation by default. Client isolation works on the understanding that a wireless device must communicate through the access point to interact with other devices on the LAN or internet. As such, some manufactures allow the option of isolating clients from each other through using the access point transceiver as a moderator.[87] In essence, this connects each device individually to the access point which stops them from detecting or interacting with each other. It has been noted how client isolation is common in most wireless access point, however, is rarely enabled by default. When this is combined with the technological illiteracy of many users, it leaves client isolation as a fringe form of protection.[88] Although far from perfect due to the ability to still attack the LAN in order to intercept data, it does prevent devices accessing the internet access point from directly attacking each other.[89] A test of a CISCO form of client isolation named PSPF highlighted how this method is effective in stopping some man in the middle attacks such as the spoofing of ARP packets.[90] What this implies is that by setting client isolation to default, numerous attacks could be prevented. In spite of the failure to stop attacks on the LAN, numerous simple attacks become redundant by implementing this feature, implying it is a beneficial added layer of security. Thus, client isolation as a default function in all guest networks could be highly beneficial in stopping certain attacks. This is particularly true considering the ease in which the feature can be

86 Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geo-location Services on Smart Mobile Devices', *Europa*, (May 2011) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf>
87 T. Mirzoev, The Role of Client Isolation in Protecting WiFi Users, p. 12
88 Ibid, p. 11
89 Ibid, p. 12
90 Ibid, p. 13

utilised.

6. New Approaches

6.1. Law Enforcement

It is hoped that the technical features highlighted here would not only protect user data, but also lessen the risks presented by law enforcement officials. When the aforementioned features are combined it should be relatively clear for law enforcement to establish whether the abuse or illicit content stems from a private or guest network. The implementation of a separate network with a separate IP address would emphasise that traffic is coming from elsewhere. When this is combined with a disclaimer it should become immediately evident that the traffic is not the hosts, and that cooperation as opposed to draconian raids would be the best option. Moreover, if the precautions previously mentioned are put in place then it is questionable as to what extent infringements would take place due to the difficulty presented. For example, a logging of the MAC and IP addresses would allow for those offering free WiFi to block those who have connected with malicious intent. This would mean that to reconnect to a connection a person would have to continually change their MAC address and IP address in order to circumvent any blocks. The same could be applied for if a resident wanted to abuse their own open connection, meaning significant labour costs would be present. When this feature is combined with the limiting of bandwidth, it adds significant time costs for anyone wishing to abuse a network. This approach offers a number of solutions which combined offer substantial protections for those sharing their connection's data, but also help prevent third party abuses making enforcement easier for police and copyright holders.

The wider acceptance of open wireless connections and Tor are reliant on a wider understanding and acceptance of the practices. This also presents a catch 22 situation as many users could be presented with uncertainty due to technically illiterate law enforcement officials or copyright holders. This itself suggests that one of the key factors alongside legislation and more effective technology is greater knowledge and awareness. There is no easy solution to this problem, but it is hoped that suggestions such as the ones forwarded within this paper would help to create awareness. This could come as a by-product of the greater use of connection sharing, necessitating more knowledge by law enforcement and copyright holders. Similarly, by using reverse DNS to show disclaimers as well as a clear split of traffic, it is hoped that police become more conscious of the differing traffic. From this it should be clear that those who share their connection are unlikely to be the perpetrators of illicit content and as such create a more civil response to breaches. Thus,

although safe harbour provisions and technical measures can minimise risk, it is still plausible for police intervention – particularly in the case of Tor exit nodes. It is hoped that these suggestion and awareness lessen the risk of possible police contact, and also any interactions would be more collaborative.

6.2. Rethinking Liability

Whilst this paper has forwarded methods which can help to maximise the protections in place for those wishing to share their internet connection, it has not stated where liability should be placed for illicit actions or copyright abuses. Liability for illicit actions such as copyright abuses should be burdened upon the person undertaking such abuses, and those people alone. Precedent for this has been set in the area of internet access providers where the burden placed on them to prevent copyright abuses is largely voluntary. The absurdity of placing liability on passive intermediaries would be comparable to holding postal services liable for the packages they deliver. As such, this paper has emphasised that the same safe harbour protections should be affirmed for other passive intermediaries such as those offering free public WiFi, or those running a Tor relay. It is vital to clearly set out these protections for those wishing to share their internet connection in order to gain the full benefits of broader and easier access to the internet. This section of the paper will emphasise why the suggestions offered in this paper could lessen the potential for overall issues of liability, but also argue that a more sustainable approach to law enforcement and copyright is necessary in conjunction with this. The issue of liability will not be covered to a great extent here as a follow up paper with a greater focus on legal nuance is necessary for this.

The e-*Privacy Directive* states that security measures taken should be proportionate to the costs related to implementation.[91] In parallel to this, the McFadden opinion prevents injunctions which terminate the internet connection, force password protections, or examine all transmitted communications.[92] When these viewpoints are combined it could be suggested that there are no methods which can be forced upon those sharing their internet connection which can reasonably prevent copyright abuses. This is because the only possible methods for ensuring no abuses take place would involve some aspect of universal monitoring which could be perceived as excessive in light of other interests such as freedom of speech and the right to privacy. In light of this any extra steps which could be taken by those offering their network connection should be voluntary – a precedent established for other passive intermediaries. This is because if the burden is voluntarily adopted then it cannot be excessive, also if only adopted by some it could be seen not to curtail

91 2002/58/EC, Article 4
92 Opinion on McFadden v. Sony, Conclusion (4)

other interests too greatly. If these measures were to be protected by a Good Samaritan provision within the Digital Single Market, then it is likely that this would curtail potential abuses to some extent. This is for the reasons mentioned within the previous section, which include blocking infected laptops or those which infringe, and for some occasions limiting bandwidth. Whilst this approach is likely to prove useful to some extent, further methods are necessary alongside this. Similarly, if these methods only were universally adopted then issues in themselves would arise in terms of net neutrality questions and broadband speeds.

6.3. Copyright

In terms of copyright infringements, the 'stick' approach which has largely been followed could be seen as ineffective. This point can be evidenced within a 2015 report by the European Commission which found website takedowns were ineffective due to the hydra-problem and the elasticity of supply.[93] Moreover, 70% of online users found nothing wrong with piracy, and 22% of global bandwidth was used for online piracy. This suggests that dealing with copyright infringements is more inherent than just enforcement of current legislation.[94] Whilst this signals that copyright infringements are widespread, it does not necessarily make them entirely damaging. A Norwegian report on copyright infringements found that those who download music illegally are also ten times as likely to pay for songs.[95] The same was re-affirmed by a Finish report which found that those who illegally downloaded films also went to the cinema and paid for home copies.[96] These, and numerous other studies highlight how copyright infringements often take place alongside other activities, with only 2% of people stating that they get all or most of their content through pirating.[97] The reasons that this anomaly occurs has been accounted to a number of reasons, with the idea of sampling the product or inaccessibility to the content two of many cited.[98] This emphasises how copyright holders should reflect inwardly on their own policies, and perhaps accept the inevitability of material being copyrighted on a small scale to some extent. If this approach were to be followed, then the problem of copyright infringements could be lessened through focusing on serious and/or

93 L. Aguiar et al., 'Online Copyright Enforcement, Consumer Behaviour, and Market Structure *Institute for Prospective Technological Studies: Digital Economony Working Paper 2015/01,* (2015), p. 1 https://ec.europa.eu/jrc/sites/default/files/JRC93492_Online_Copyright.pdf

94 Enigmax, '70% of the Public Finds Pirating Acceptable', *Torrentfreak,* (February 2011) <https://torrentfreak.com/piracy-socially-acceptable-110228/>

95 S. Michaels, 'Study Finds Pirates 10 Times More Likely to Buy Music', *Guardian* (April 2009) <https://www.theguardian.com/music/2009/apr/21/study-finds-pirates-buy-more-music>

96 S. Gibbs, 'Piracy Study Shows Illegal Downloaders are More Likely to Pay for Films Than Music', *Guardian* (May 2014) <https://www.theguardian.com/technology/2014/may/06/piracy-film-music-study-pay-illegal-download-damage>

97 'Copy Culture: Overall Trends', *American Assembly Columbia University,* <http://piracy.americanassembly.org/copy-culture-report/copy-culture/>

98 P. Belleflamme, 'The Hidden Treasure of Piracy?', *IPdigIt,* (December 2013) <http://www.ipdigit.eu/2013/12/the-hidden-treasure-of-piracy/>

serial infringers. This would also stop unreasonable burdens being placed on those sharing their connection.

6.4. Unnecessary Technology

A more difficult problem, which requires more innovative solutions is presented in terms of illicit content and law enforcement. This content can range from issues such as drugs being sold on onion services, to problems like revenge porn. As previously mentioned, this report will not propose a universal solution for the problems created through balancing interests, rather, it will offer pointers as to where possible approaches could lie. In essence, for privacy and anonymity to be preserved to the greatest extent it can, law enforcement agencies need to employ smart and reasonable approaches. It has often been proved that law enforcement agencies can catch people through traditional detective work without any other technical features.[99] For example, in the case of something like revenge porn, there are already a limited number of suspects, so with a warrant it would generally be relatively easy to catch the initial source of the material. Similarly, even for cases such as online narcotic sales where a set of initial suspects cannot be formulated, various factor can be examined in order to narrow the list down. This could be done through similar content being uploaded from open hotspots in a certain areas, or linguistic features within postings.[100] Likewise, if a specific router is continually being flagged as producing undesirable content, then the police could look at the forensics of the device. What this suggests is that technology should not be considered the only option for catching those misusing shared internet, as traditional tools can often be effective. This is not to say that technical approaches should be completely disregarded. In certain occasions it could be beneficial to exploit flaws in the Tor browser, or to monitor and hack in a targeted fashion. When they are deemed necessary these technical intrusions could be employed by police, but would need to be done as a last option and with significant levels of oversight. Although there is a possibility that following this method would slow down the police effort, it would ensure the correct levels of scrutiny were being employed and that irrelevant technical measures were not used for the sake of themselves.

Conclusion

99 A. Grossman, 'Federal Agents Pierce Tor-Anonymity Tool', *Wall Street Journal*, (April 2014) <http://www.wsj.com/news/articles/SB10001424052702303949704579461641349857358?mod=WSJ_TechWSJD_NeedToKnow>

100 A. Crenshaw, Dropping Docs on the Darknet: How People Get Caught, https://www.defcon.org/images/defcon-22/dc-22-presentations/Crenshaw/DEFCON-22-Adrian-Crenshaw-Dropping-Docs-on-Darknets-How-People-Got-Caught-UPDATED.pdf

This essay has sought to examine how to promote greater connection sharing in the residential sphere, namely, through making the process safer and clearer. The importance of this examination stemmed from the benefits which can be gained from connection sharing, a feature briefly touched upon within this paper. These include the empowering effects that can be had for individuals, the privacy such connections can provide and the benefits presented to business. In order to benefit from these features, a series of legal and technical measures were forwarded within these paper. These suggestions are to be read in conjunction with each other due to the necessity of a rounded solution in resolving the risks presented by connection sharing.

The first section within this paper pointed towards the inherent risks present within current connection sharing. One of the major risks highlighted came from the damage third party traffic could cause, with a broad range of consequences possible from this. The most likely of these was a termination of the IAP contract – a factor which can be accounted to the fact that most acceptable usage policies are not tolerant of connection sharing, or place liability on the person sharing their connect. Moreover, even if an IAP is found who is accepting of this, issues arise from confusion over whether the traffic originates from the primary user, or a guest. A result of this is the possibility of civil lawsuits arising from either confusion or the desire to enact a preventative injunction. Although a McFadden ruling may play a part in mitigating some confusion, it is unlikely to be full-proof because of its vagueness in the area of preventative injunctions and its focus on national interpretation. Finally, the possibility of law enforcement issues are still present, a particularly salient factor for those sharing their connection in the form of a Tor exit node. If traffic coming from a third party is illicit and is not distinguished from private traffic then police raids or the seizure of servers is possible. These varying levels of repercussions highlight how the confusion presented by third party traffic could leave those who share their connection at risk, whilst dissuading others from doing so.

The technical risks presented by sharing a router were also stated. These risks tended to focus on the access people can gain to personal data from inherent weaknesses in encryption and protection. Eavesdropping applications such as *Firesheep* or *Fing* offer amateur hackers the chance to perform basic session hijacking and port sniffing attacks. These sorts of attacks leave unencrypted data vulnerable and could result in some personal details being revealed. More complex attacks which can circumvent higher levels of encryption such as ARP spoofing are also possible and allow damaging personal details such as banking information to be accessed. Alongside eavesdropping, access to files is often also possible because of weak firewall protections on personal networks. This can leave shared files and devices both visible and accessible to those with malicious intent if

sufficient protections are not put in place. A result of these weak protections also leaves scope for malware infection which could spread on to multiple machines connected to the network. When these technical weaknesses are combined with the legal risks previously mentioned, it leaves numerous inherent risks present for those wishing to share their internet connection.

This paper sought to combine legal and technical solutions in order overcome a number of the issues present. In order to establish legal protections, it was argued that specific legislation within the Digital Single Market initiatives would be advisable. This would come in the form of affirming the position of those sharing their internet connection as a mere-conduit, in turn establishing the same safe-harbour provisions present for IAPs. It was also suggested that this should be combined with a Good Samaritan Clause which prevents punitive measures for taking voluntary legal measures which offer protections to consumers (and potentially copyright holders). Legislation of this sort would affirm that those who share their internet connection are not liable for the traffic over their network, or any measures they take to prevent undesirable traffic. An effect of this would be greater clarity for those wishing to share their connection that they are not going to be taken to court for offering a public good. If this was combined with an acceptable usage policy by IAPs which allows for connection sharing, then from a theoretical legal perspective the risks would be minimal (or non-existent).

In order to materialise this theoretical risk alleviation, an improvement in the technological features commercially available would be necessary. Various different features could help mitigate both legal confusion and also the technical risks which connection sharing creates. The most important of these is splitting router traffic by default through having two separate IP addresses. This would allow for a clear dichotomy between private and public traffic – lessening both third party confusion and malicious attacks towards private networks. This feature could act as a base from which various other features could be used to help clarify the split, and also offer technical protection. For example, the split in traffic could be further clarified through a list of public connections which is accessible to those who were effected by the shared connection. This transparency of purpose could also be maximised by a reverse DNS stating that the router is a shared connection. If this were to be implemented then it should become obvious to civil parties and law enforcement (amongst others) as to what the purpose of the connection is. This would facilitate a more constructive and collaborative approach. Finally, through offering further features such as client isolation, MAC address blocking and bandwidth controls the amount of malicious behaviour could be decreased. Combined, these features allow malicious users to be largely isolated, unable to upload large amounts and also blockable for if they circumvent these protections.

When the legal and technical features suggested in this paper are combined, the risks present from connection sharing can be perceived as decreased significantly. If all the suggestions in this paper were implemented then numerous stakeholders could benefit, especially those who wish to share their internet connection. This is because the aforementioned suggestions minimise any direct risks posed to them by malicious users, civil parties and also law enforcement. Alongside this, those wishing to access internet connection could not only gain the benefits of more open connection points, but also hotspots which are better defended against attackers. Finally, law enforcement and civil parties could gain from the greater clarity produced over who is infringing, and as such follow a more precise and effective investigation of serious and/or serial infringers. This essay has also sought to emphasise that in order to achieve these benefits a multifaceted approach is needed. Both technical and legal aspects need to be resolved in order to establish safe and clear internet sharing, and to do this input from different parties is needed. In order to start this catalyst of safer and clearer connection sharing, a focus within the Digital Single Market is necessary – with a particular focus on clarifying mere-conduit safe-harbours advisable. Likewise, from a technical perspective, the further stimulation of split IP addresses within routers could extensively improve the protection of those offering to share their connection. Thus, the benefits of promoting these two features amongst others could be beneficial to numerous stakeholders in the medium to long term.

Whilst this paper has forwarded many recommendations surrounding connection sharing and how to alleviate risk, it has also created a number further questions. For the policy recommendations forwarded within this paper to be successful, further follow up papers would be advisable to clarify certain points. The most important of these is fully addressing the issue of liability which arises from connection sharing. Whilst this paper touched on some suggestions for how to approach liability, it did not offer an extensive examination into this. As such, the broader investigation in to connection sharing would benefit from a paper which specifically seeks to address how to coalesce connection sharing and attributing liability to the infringing individual. Within this, it would also be beneficial to examine the burdens which are placed on internet access providers and consider whether any would/should be applied to those sharing their connection.

Bibliography

Bibliography

Academic Papers

- Busch C., Secondary Liability for Open Wireless Networks in Germany: Balancing Regulation and Innovation in the Digital Economy, SSRN, (2015)
- 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censorship, Penn America, (2013)
- Mirzoev T. & White S., The Role of Client Isolation in Protecting WiFi Users from ARP Spoofing Attack, I-managers Journal on Information Technology (2014)
- Schellekens M., 'The Internet Access Provider: Unwilling or Unable', International Journal of Law and Information Technology (2015)
- 'Tainted Love: How WiFi Betrays Us', F-Secure (2014)
- Taylor S. et al, 'What Do Consumers Want from Wifi', CISCO, (2012)
- Van der Sloot B., 'Welcome to the Jungle: the Liability of Internet Intermediaries for Privacy Violations in Europe', Journal of Intellectual Property, Information Technology and Electronic Commerce Law, (2015)
- van Eijk N. et al, 'Moving Towards Balance: A Study Into Duties of Care on the Internet', IViR (2010)

Case Law

- Judgement of the Court: UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH, Curia, (March 2014)
- L'Oreal SA & Others v EBay International AG & Others, (July 2011)
- Opinion of Advocate General Szpunar: Tobias McFadden v. Sony Music Entertainment Germany GmbH, (March 2016)

Legislation and Treaties

- Directive 2000/31/EC
- Directive 2001/29/EC
- Directive 2002/58/EC
- Regulation 2016/679/EC

- *Treaty of the Functioning of the European Union* (2007)

European Reports

- Aguiar L. et al., 'Online Copyright Enforcement, Consumer Behaviour, and Market Structure Institute for Prospective Technological Studies: Digital Economony Working Paper 2015/01, (2015), p. 1 https://ec.europa.eu/jrc/sites/default/files/JRC93492_Online_Copyright.pdf
- Article 29 Data Protection Working Party, 'Opinion 13/2011 on Geo-location Services on Smart Mobile Devices', Europa, (May 2011) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf>
- ‘Commission Updates EU Audiovisual Rules and Presents Targeted Approach to Online Platforms', EU Commission, (May 2016) <http://europa.eu/rapid/press-release_IP-16-1873_en.htm>
- 'Commission to Boost Europe's Defences Against Cyber-Attacks, European Commission (September 2010), <http://europa.eu/rapid/press-release_IP-10-1239_en.htm?locale=fr>
- Cybersecurity Strategy of the EU: An Open, Safe and Secure Cyberspace, EU Commission, (February 2013)
- 'Digital Single Market: Roaming', EU Commission, (April 2016) <https://ec.europa.eu/digital-single-market/en/roaming>
- ‘Digital Single Market: The Strategy', EU Commission, (February 2016) <https://ec.europa.eu/digital-single-market/digital-single-market>
- 'Europe Loves WiFi: New Study Recommends More Spectrum Should be Available', European Commission, (August 2013) <http://europa.eu/rapid/press-release_IP-13-759_en.htm>
- 'Summaries of Important Judgements', EU Commission <http://ec.europa.eu/dgs/legal_service/arrets/10c070_en.pdf> (May 2012)

News Articles

- Belleflamme P., 'The Hidden Treasure of Piracy?', IPdigIt, (December 2013) <http://www.ipdigit.eu/2013/12/the-hidden-treasure-of-piracy/>

- Burgess B., 'Keep Your Windows Computer Secure on Public Wireless Hotspots, How to Geek, (August 2010) <http://www.howtogeek.com/howto/26674/keep-your-windows-computer-secure-on-public-wireless-hotspots/>
- Collins B., 'Ofcome Warns off Free WiFi Providers', Alphr, (2010) http://www.alphr.com/news/security/358342/ofcom-warns-off-free-wi-fi-providers
- Cox J., 'The People who Risk Jail to Maintain the Tor Network', Motherboard, Vice (April 2015) <https://motherboard.vice.com/read/the-operators>
- E. Butler, 'Firesheep', Codebutler, (October 2010), <http://codebutler.com/firesheep/>
- Enigmax, '70% of the Public Finds Pirating Acceptable', Torrentfreak, (February 2011) <https://torrentfreak.com/piracy-socially-acceptable-110228/>
- Gibbs S., 'Piracy Study Shows Illegal Downloaders are More Likely to Pay for Films Than Music', Guardian (May 2014) <https://www.theguardian.com/technology/2014/may/06/piracy-film-music-study-pay-illegal-download-damage>
- Grieshaber K., 'German Court Orders Wireless Passwords for All', NBC News, (December 2010) http://www.nbcnews.com/id/37107291/ns/technology_and_science-security/
- Grossman A., 'Federal Agents Pierce Tor-Anonymity Tool', Wall Street Journal, (April 2014) <http://www.wsj.com/news/articles/SB10001424052702303949704579461641349857358?mod=WSJ_TechWSJD_NeedToKnow>
- Hoffman C., 'HTG Explains: Why you Shouldn't Host an Open WiFi Network', How to Geek, (August 2013) <http://www.howtogeek.com/132925/htg-explains-why-you-shouldnt-host-an-open-wi-fi-network/>
- Jackson M., '1 in 3 Routers to Double up as Public Hotspots by 2017', ISPreview, (January 2016) http://www.ispreview.co.uk/index.php/2016/01/1-in-3-home-broadband-routers-to-double-as-public-wifi-hotspots-by-2017.html
- Janik T., 'Tor Exit Node for Less Than a Week', Testbit, (June 2013) <https://testbit.eu/tor-exit-node-less-week/>
- Kaste M., 'When a Dark Web Volunteer Gets Raided by the Police', NPR, (April 2016) <http://www.npr.org/sections/alltechconsidered/2016/04/04/472992023/when-a-dark-web-volunteer-gets-raided-by-the-police>
- Lawson K., 'Are Your Shared Files at Risk on a Hotel Network?', Private WiFi (November 2011) <http://blog.privatewifi.com/are-your-shared-files-compromised-on-a-hotel-wifi-network/>
- Leersen P., Lots to Like in Advocate General's Opinion on Free WiFi and Copyright, EDRI,

(March 2016) <https://edri.org/lots-to-like-in-advocate-generals-opinion-on-free-wifi-copyright/>

- Michaels S., 'Study Finds Pirates 10 Times More Likely to Buy Music', Guardian (April 2009) <https://www.theguardian.com/music/2009/apr/21/study-finds-pirates-buy-more-music>
- Pauli D., 'Austrian Tor Exit Relay Operator Guilty of Ferrying Child Porn', The Register, (July 2014) <http://www.theregister.co.uk/2014/07/04/austrian_tor_exit_relay_op_found_guitly_for_ferrying_child_p0rn/>
- Porter T., 'Paedophiles and Criminals Using Open WiFi Networks, Warn Police', International Business Times, (February 2014) <http://www.ibtimes.co.uk/paedophiles-criminals-using-open-wi-fi-networks-warn-police-1434820>
- Ram A., 'Smartphones Bring Solace and Aid to Desperate Refugees', Wired, (May 2015)
- Rose N. & Potts B., 'Leaked Commission Communication – No Change for Intermediary Liability Regime', Lexology, (May 2016) <http://www.lexology.com/library/detail.aspx?g=4f7749dc-a1b6-4814-9aa6-6e2385e0ce85>
- Zorz Z., 'Google Starts Tracking, Encourages Worldwide HTTPS Usage', Helpline Security, (March 2016) <https://www.helpnetsecurity.com/2016/03/16/worldwide-https-usage/>
-
- Online Resources:
- '47 U.S. Code Section 230 - Protection for Private Blocking and Screening of Offensive Material', Cornell University Law School, <https://www.law.cornell 'Copy Culture: Overall Trends', American Assembly Columbia University, <http://piracy.americanassembly.org/copy-culture-report/copy-culture/>.edu/uscode/text/47/230>
- 'About BT WiFI, BT, <https://www.btwifi.co.uk/>
- Crenshaw A., Dropping Docs on the Darknet: How People Get Caught, https://www.defcon.org/images/defcon-22/dc-22-presentations/Crenshaw/DEFCON-22-Adrian-Crenshaw-Dropping-Docs-on-Darknets-How-People-Got-Caught-
- ‘Legal FAQ’, Tor, (April 2014) <https://www.torproject.org/eff/tor-legal-faq.html.en>
- Lenhardt J., 'Friefunk Statt Angst', (July 2012), <http://writing.jan.io/2012/07/26/freifunk-statt-angst.html>
- Open Wireless Movement, <https://openwireless.org/routers>
- Scott T., 'Policy to Require Secure Connections Across Federal Websites and Web Services',

Executive Order of the President, (June 2015) <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf>

- 'Statistics and Market Data about E-Commerce', Statista https://www.statista.com/markets/413/e-commerce/
- ‘The Zettabyte Era' – Trends and Analysis, CISCO, (June 2015) <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html>
- 'Tor Metrics – Relays and Bridges in the Network', Tor <https://metrics.torproject.org/relayflags.html?start=2011-03-07&end=2016-06-05&flag=Running&flag=Exit&flag=Guard>
- 'Tor Overview', Tor https://www.torproject.org/about/overview
- 'Understanding the WPA2 'Hole 196' Attack: Vulnerabilities & Motorola WLAN Countermeasures', Motorola (2010) <http://www.airdefense.net/whitepapers/UnderstandingWPAWPA2Hole196Attack_TB_0810_chv4.pdf>
- 'Viruses, Spyware and Malware', Information Systems and Technology, https://ist.mit.edu/security/malware