GLOBAL PARTNERS DIGITAL June 2014

STATE OF EVIDENCE: The Economic Impact of a Human Rights-Based Internet

EDITED BY **GLOBAL PARTNERS** DIGITAL

GLOBAL PARTNERS DIGITAL

June 2014

STATE OF EVIDENCE: The Economic Impact of a Human Rights-Based Internet

BY DANIEL KENNEDY

gp-digital.org

Global Partners Digital
Development House
56–64 Leonard Street
London
EC2A 4LT
+44 (0)207549 0337
info@gp-digital.org
gp-digital.org

Global Partners & Associates Ltd
Registered in England and Wales

Company Nº 520 1603
VAT Nº 840 1912 54

CONTENTS

EXECUTIVE SUMMARY

There is extensive research demonstrating that increased internet usage and penetration spurs economic growth, increases competitiveness and innovation, attracts foreign investment and creates jobs. This relationship has been accepted by policymakers across the world, resulting in the implementation of more and more schemes to increase internet access and use. Beyond this it is often argued that countries with a free and open internet environment, where online human rights are protected and upheld, experience greater economic benefits than those countries with an internet that is overly regulated or where human rights are not protected. If this relationship is proven and accepted it could have a significant impact on approaches to internet policy-making. Despite this, until recently there has been very little research into the relationship between the nature of the internet environment and its economic impacts.

This paper takes four key policy issues for protecting human rights online - net neutrality; an absence of arbitrary online filtering and blocking; an absence of arbitrary surveillance; and protecting intermediaries from liability for user-generated content. For each policy area it summarises the theoretical economic arguments for adopting a human rights-respecting position, and then attempts to collate any empirical data that exists to back up those arguments. In doing so, the paper aims to assist human rights defenders to develop persuasive arguments that they can use with policy-makers, and to highlight areas where more research and evidence is needed.

The paper finds that there are extensive theoretical arguments that human rights defenders can draw upon regarding the economic benefits of protecting human rights online, but the empirical evidence is very sparse and further research is needed.

Of all the issues examined, **network neutrality** was the most extensively studied. There is empirical research to counter many of the arguments for not protecting network neutrality – the evidence suggests that network neutrality does not discourage internet service providers from investing in infrastructure, and there is little indication that net neutrality would inflate consumer prices. On the other hand there is evidence to suggest that without net neutrality, the 'network effect' (in which networks become more valuable the larger they are) would be diminished, thus decreasing the overall economic value of the internet. If large content and service providers were able to pay for users to have privileged access to their content, the entry costs to the market for newcomers would increase with a corresponding stifling effect on competition.

There is data from Australia suggesting that a proposed **blocking and filtering** system would have a deleterious effect on broadband speeds (which are closely linked to economic performance). This is on top of the costs of implementing the system which were estimated at AUS $45 million in initial investment and AUS $33 million in yearly operating costs. In China too, despite a massive online economy, local start-ups surveyed complained of a loss of productivity that comes from having to bypass the 'great firewall' to do business with or access foreign sites.

Research into the economic effects of **online surveillance** has centred on the fallout from the Snowden revelations. The evidence demonstrates that

US companies have already been negatively affected as foreign clients show increased fear that their data may be accessed by the US government without their knowledge or consent. 56% of non-US respondents to a survey on the PRISM revelations said they are now less likely to use US-based cloud providers. Another report estimates that US companies could suffer a loss of up to 20% in foreign markets, translating to a loss of USD $35 billion by 2016. Less directly, many analysts predict that some states respond to the crisis in trust by passing laws requiring data about their citizens to be stored on their territory, and this could also harm the 'network effect' and require large financial resources to implement.

A review of the literature on **intermediary liability** shows that where the limits of intermediary liability are either poorly defined, or too onerous, content and service providers can be discouraged from operating or forced to bear excessive legal costs. Research showed this is especially true in two states, Turkey and Thailand, which both have very strict intermediary liability regimes. In Thailand's case, the potential liabilities arising from the restrictive 'Act on Computer Crime' are likely costing investment due to the presence of more liberal regimes in the region.

While these studies are important and should be drawn upon to ground advocacy claims, it is clear that much more study is needed in to the economic impact of protecting human rights online. Research to date has predominantly focused on the large and relatively developed economies of the G20. It would be valuable to examine the extent to which these trends hold true and can be evidenced in developing countries. The relationship between foreign direct investment in the internet industry and the extent to which a state respects human rights online could be a fruitful line of inquiry for further research. Indicators such as number of start-ups and the development of internet exchange points within states could also be useful in gauging how a human rights-based approach to internet governance affects a state's economy.

INTRODUCTION

It is a truth universally acknowledged that increased internet usage and penetration spurs economic growth, increases competitiveness and innovation, attracts foreign investment, and creates jobs. This contention is backed up by a large amount of economic research and data, and has been accepted by policymakers around the world. A commonly held corollary of this contention is that a free and open internet, governed by a normative respect for human rights, spurs faster growth and provides greater economic benefits than an internet that is overly regulated by the state or other actors. This is taken as a given by many, especially by policymakers concerned with combating censorship and excessive regulation of online activity, and promoting principles such as net neutrality and freedom of expression. The president of the Information Technology Association of the Philippines, Dondi Mapa, for instance, was widely quoted in the run-up to the 2012 World Conference on International Telecommunications in Dubai as saying:

> 'The Internet has become a 21st-century trading route. Regulating the Internet's openness may take away the innovation, creativity and dynamic growth that has contributed immensely to the global economy, and has helped shape the economies of developing countries such as the Philippines and India.''

Despite the popularity of this narrative, there has been surprisingly little research done into the actual effects of different approaches to internet governance on the economy until relatively recently. A January 2014 report by the Boston Consulting Group, *The Connected World: Greasing the Wheels of the Internet Economy* attempted to identify and quantify sources of 'e-friction' – factors that prevent states from taking full economic advantage of the internet. The methodology used data from *Freedom on the Net* and the P*ress Freedom Report* as well as the Open Net Initiative's filtering score, to weigh a state's e-friction in the 'information' category, though other factors such as availability of content in the state's users' language were also weighed. *Open for Business: The Economic Impact of Internet Openness,* a March 2014 report from the Dalberg Group, similarly noted that there was a strong correlation between states that promoted openness[1] in their internet policy and the contribution of the internet to their gross domestic product (GDP). The paper drew on both quantitative analysis and primary qualitative research, including interviews with 30 experts and practitioners, comprising of 'academics, government officials, ICT company executives, entrepreneurs, investors, and advocates.' It also collated information from over 60 existing studies, including Freedom House's *Freedom on the Net* index and a number of economic indicators including GDP and the level of online economic activity.

This paper attempts to investigate to what extent economic arguments can be made in favour of a human rights-based internet. It looks at several of the key elements of a human rights-based internet including net neutrality, an absence of arbitrary online filtering and blocking or surveillance by governments and protecting intermediaries from liability for user-generated content, and attempts to draw together economic arguments that have been made in favour of these policies. In addition to looking at the theoretical economic arguments in favour of these policies, it also attempts to collate empirical data from research, in order to establish what evidence exists on the economic impact of these policies. By collating and arranging the information in this way, this report aims to serve as a resource for advocates of a human rights-based internet.

SCOPE: DEFINING A HUMAN RIGHTS-BASED INTERNET?

The contention that a free and open internet has a positive economic impact requires that a 'human rights-based internet' first be defined, or at least approximated. This report has drawn on the recommendations of the 2011 *Report of the Special Rapporteur on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet* to establish some of the criteria for a human rights-based internet. However, it is not an extensive or definitive explanation of how such an internet can be achieved and a human rights-based internet may cover issues that are beyond the scope of this report. While some policies are intrinsic to a human rights-based internet - such as protecting intermediaries from liability for user-generated content or an absence of blocking and filtering except in very narrow circumstances - are relatively uncontested, net neutrality is a much more complicated issue. While to some it is the very cornerstone of a free internet, to others, it represents unwarranted and harmful government intervention in the free market. As such this paper has attempted to examine the economic arguments and evidence both in favour of and against net neutrality.

Although there are clear moral justifications for a human rights-based internet, and many of the principles that underpin such an internet are enshrined in international law, if there are indeed economic arguments and evidence for a human rights-based internet, then human rights defenders could consider using them, particularly when advocating to actors who are less susceptible to human rights-based arguments.

NET NEUTRALITY

Net neutrality is defined by Tim Wu, who coined the term, as 'the idea… that a maximally useful public information network aspires to treat all content, sites, and platforms equally. This allows the network to carry every form of information and support every kind of application.' The idea is sometimes referred to as the 'end-to-end principle' or the 'dumb pipes' principle. In crude terms, it means that a network (in the debate, usually that provided by an internet service provider) should not discriminate in terms of the type of traffic it carries and treat everything, from email to peer-to-peer (p2p) traffic to online video streaming to Voice over Internet Protocol (VoIP), equally. In reality, however, even strong advocates of net neutrality like the Center for Technology and Democracy concede that 'appropriate exceptions should be made for reasonable network management.'[2]

Arguments over net neutrality hinge on the question of the right of individuals to freely access and disseminate information online. Proponents of net neutrality believe that should internet service providers (ISPs) have the ability to block or slow down certain types of traffic, they will either restrict access to or compel intermediaries and users to pay premium tariffs to ensure their content and services that are not in their economic interests, services or content are privileged.

This would fundamentally alter the ability of the internet to be a means for expression and information access. An ISP could, in theory, restrict access to sites or sections of the internet if its customers (or the sites themselves) do not pay a higher fee for access.

BLOCKING AND FILTERING

Governments block access to online content for a variety of reasons including to prevent children, and in some countries adults, from accessing content deemed obscene, to prevent online piracy and uphold intellectual property rights, even to prevent people from connecting and mobilising online. The global

nature of the internet, where content created or stored in one jurisdiction can easily be accessed by users in another, means states have come to increasingly rely on online filtering in an effort to prevent users in their jurisdiction from accessing content they deem "undesirable" that is hosted abroad. While states are allowed, under international human rights law, to limit access to content, such limitations are only allowed in narrow and well-defined circumstances, as outlined in article 19 of International Covenant on Civil and Political Rights. The 2011 *Report of the Special Rapporteur* lays out the test for whether filtering or blocking complies with human rights standards:

> (a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency); and
>
> (b) It must pursue one of the purposes set out in article 19, paragraph 3, of the Covenant, namely (i) to protect the rights or reputations of others, or (ii) to protect national security or of public order, or of public health or morals (principle of legitimacy); and
>
> (c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).

Even blocking and filtering regimes that limit expression not protected under international law (such as child abuse imagery) are often problematic because of a lack of transparency about what content is blocked and the processes by which that determination is made or because the deciding body is not a competent judicial authority.

ONLINE SURVEILLANCE

Since news broke of the US National Security Agency's surveillance programme, PRISM, in June 2013, the need to balance security and privacy concerns online has become possibly the most contentious and widely discussed internet governance question today. Online surveillance can lead to a violation of the right of the individual to privacy, which is guaranteed under article 12 of the *Universal Declaration of Human Rights* and article 17 of the International Covenant on Civil and Political Rights. The right to privacy may be limited, under international law, to achieve certain legitimate aims. However the *Report of the Special Rapporteur* stresses that

> ''Measures encroaching upon this right must be taken on the basis of a specific decision by a State authority expressly empowered by law to do so, usually the judiciary, for the purpose of protecting the rights of others, for example to secure evidence to prevent the commission of a crime, and must respect the principle of proportionality(...)''

The report also stresses that states have a responsibility to enshrine 'through clearly articulated laws, principles and procedures regarding 'the recording, processing, use and conveyance of automated personal data and to protect those affected against misuse by State organs as well as private parties.'

INTERMEDIARY LIABILITY

'Internet intermediaries' are a broadly defined set of online services, which includes ISPs, search engines, blogging platforms, social networks, online payment systems, and e-commerce platforms like Amazon and eBay. A useful definition of 'internet intermediaries', provided by a 2010 Organisation for

Economic Co-operation and Development (OECD) report, *The Economic and Social Role of Internet Intermediaries*, is services that 'give access to, host, transmit and index content originated by third parties or provide Internet-based services to third parties.' Freedom of expression concerns arise when these services are held liable for third party activities or content that is hosted or transmitted on their networks.

As the 2011 *Report of the Special Rapporteur* argues, protecting intermediaries from liability for user-generated content is one of the cornerstones of a human rights-based internet as

> ''holding intermediaries liable for the content disseminated or created by their users severely undermines the enjoyment of the right to freedom of opinion and expression, because it leads to self-protective and over-broad private censorship, often without transparency and the due process of the law.''

A reasonable regime that limits the liability of intermediaries for user-generated content is therefore necessary to protect online freedom of expression.

NOTES

1. 'Openness was as respect for four principles: freedom, interoperability & equity, transparency, and security & privacy.
2. 'Openness was as respect for four principles: freedom, interoperability & equity, transparency, and security & privacy.

ECONOMIC BENEFITS OF THE INTERNET

THE ARGUMENT

The internet is widely held to provide numerous economic benefits to the individual, businesses, and to states. Much of this stems from the ability of the internet to connect people from all around the world, lowering transactional costs between them and allowing for increased economic efficiencies. As the Boston Consulting Group (BCG) argues in a 2014 report, *The Connected World: Greasing the Wheels of the Digital Economy,*

> ''Restrictions on international trade inevitably make both sides poorer, Adam Smith declared in 'The Wealth of Nations' in 1776. His observation holds true today even though Smith could not have imagined the industrial, communications and digital revolutions that have shaped the intervening two and half centuries.''

The benefits of increased online trade exist not only between states, but also within them. Increased access to information lowers costs and increases competition, spurring trade on the national level too. The internet lowers the barriers to entering the market considerably for a large number of economic activities. For example, while traditionally a retailer would need to have the capital to purchase premises in order to sell goods to customers, the internet enables people to sell many types of goods directly, dramatically lowering the cost of entering the market.

In addition to spurring trade, the internet also facilitates a plethora of services that would not be possible in the pre-digital age, such as cloud storage of data, inexpensive VoIP communication, highly-targeted advertising, access to cultural and educational materials through downloads and streaming, and real-time information on almost every conceivable market. These services not only increase efficiencies, they employ large numbers of people and are an important economic sector in and of themselves.

SUPPORTING STUDIES AND LITERATURE

The economic impact of increased internet penetration and speed has been widely and comprehensively examined. A 2012 literature review by the Markle Foundation, *The 3 Billion Question: Does the Internet accelerate Economic Growth* found a strong positive correlation between these factors and increased GDP and employment. According to the review studies show that:

- Every 10 percentage point increase in broadband penetration increases GDP by 1%.
- A study of 27 developed and 66 developing countries, found that al1 percentage point increase in the number of internet users is correlated with a boost in exports of 4.3 percentage points.
- Doubling the broadband speed for an economy increases GDP by 0.3%.
- In 2010, ICT services employment in OECD countries grew by 18% while employment growth in business services was 12%.

The economic impact of the internet at the national level has also been examined in a number of studies. A 2010 study by BCG entitled *The Connected Kingdom, How the Internet is Transforming the UK Economy* found that in 2009, the internet contributed a full 7.2% to the British gross domestic product and that it was expected that this share would rise to 10% of GDP by 2015. The report noted that were the internet economy considered a separate economic sector, it would be the nation's fifth largest, more important than construction or health and social work. The report noted the importance of the internet to the British economy stemmed from a strong e-commerce market, which was the largest in the world per capita.

Internet Matters: The Quiet Engine of the South African Economy, a 2013 study by World Wide Worx found that adding together e-commerce, internet access and presence, online advertising, investment in data infrastructure and government spending on broadband infrastructure, the internet contributed 2% of South Africa's GDP in 2011.

The UK and South Africa are not alone in reaping the economic benefits of the digital age. A 2012 publication from BCG entitled *The $4.2 Trillion Opportunity: The Internet Economy in the G20* found that in 2010 the internet sector contributed a total of 4.1% to the GDP of the G20 economies. This benefit, however, was not evenly shared across different states. While the internet sector accounted for 8.2% of the UK's GDP and 4.7% of the USA's, it contributed only 2.2% of Brazil's GDP and only 1.3% of Indonesia's. The report projected the difference in the impact of the internet on developed and developing economies to narrow slightly by 2016. If in 2010 the internet contributed 4.3% to the economies of the G20's developed states but only 3.6% to the economies of its developing markets, by 2016 the figures were expected to be 5.5% and 4.9% respectively. The report also predicted South Africa's internet sector would increase from 1.9% to 2.5% over the same period, a figure that seems to have been corroborated independently in the Word Wide Worx study cited above.

The internet's contribution to growth in GDP is also increasing year on year. A 2011 McKinsey Global Institute report, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity* found that the internet accounted for 10% of GDP growth over the past 15 years in 13 developed economies but that over the past five years, the internet's contribution to GDP growth in these countries doubled to 21%.

NET NEUTRALITY

THE ARGUMENTS

Net neutrality (or network neutrality) holds the distinction of being perhaps the most empirically examined and contentious of all the policies examined in this paper. Nevertheless, research has tended to focus on the US telecommunications market, which detracts from the universality of the evidence available.

Primarily, in the economic sphere, support for net neutrality stems from fears that carriers will leverage their market positions to promote, block or slow down access to content to privilege content they themselves have an economic stake in. This in turn would freeze out smaller competitors and stifle innovation. There is also the concern that unless net neutrality is enshrined as a principle of governance, it will lock less powerful actors both in developed economies and in the global South out of the market, as they will be unable to afford the costs of access to privileged networks. Start-ups and small and medium enterprises both in the west and in the global South may lack the capital to ensure providers allow or privilege access to their content or services. This will exacerbate the pre-existing digital divide and prevent less powerful actors from taking advantage of the economic benefits of increased interconnectivity. For proponents of net neutrality, enshrining it as a governance principle is crucial to ensuring a level economic playing field.

Conversely others argue the effects of net neutrality are overstated or that arguments in favour of net neutrality stem from hypothetical worst-case scenarios that are not probable in the real world. In a 2008 paper entitled *The Economics of Net Neutrality Revisited,* Gernot Pehnelt argues that market forces would constrain ISPs from unduly restricting access to content and that the European Union's powerful anti-trust laws would be sufficient to prevent a monopoly arising.

Outside of moral questions of the ability or right of ISPs to regulate or restrict access to internet content, the debate hinges on a number of economic issues including competitiveness, market regulation, consumer pricing, and encouraging investment in infrastructure and innovation. Opponents argue that net neutrality prevents ISPs from tailoring their services to their customers and thus inhibits competition and innovation. Proponents argue it ensures intermediaries can compete on a level playing field. Opponents argue it will allow lower income users to choose a service that suits their limited needs, proponents argue it increases the digital divide. Opponents argue it discourages investment in broadband infrastructure, as a return on investment is not guaranteed, proponents argue that history shows little evidence ISPs make investment decisions this way.

Given the intensity of the debate, an examination of the evidence for the real economic effects of network neutrality is essential.

SUPPORTING STUDIES AND LITERATURE

ISPs in the American market have overwhelmingly opposed net neutrality regulations, arguing that they would discourage investment in broadband infrastructural and/or increase consumer prices. This position is best

exemplified in a 2010 report by Stratecast, a telecommunications research company in the US. *Net Neutrality: Impact on the Consumer and Economic Growth* looks at three potential models of regulation: 'status quo' (The FCC's four principles [3] would be how most companies do business), 'narrow non-discrimination' (the four principles would be enshrined in regulation) and 'strict non-discrimination' ('a completely bit-agnostic approach to network design and management') and examines the potential effects these regulatory frameworks would have on innovation, prospective revenue, non-access service revenue, the costs of regulatory compliance and infrastructure roll-out.

The report argues that while 'narrow net neutrality' would only increase the costs of regulatory observance, 'strict net neutrality' would remove the ability of broadband providers to charge for premium services, reducing prospective revenue and discouraging the rollout of broadband where a return on investment could not be guaranteed. Unable to gain revenue except on the basis of access, the cost to consumers could be an extra $10 to $55 a month on top of their normal average payment of $30. The report argues that strict net neutrality would also increase operating costs for the nation's providers from $20 billion to $40 billion annually and that 'these costs would come from increased [capital expenditure] to overbuild the network to accommodate increased demand without the benefits of [quality of service] technologies.' A knock on effect from this loss of investment would be that 'non-network service providers' such as Google, Facebook and Amazon, who depend on the increased infrastructure investment of providers to grow, would lose out on anywhere from $20 billion to $100 billion between 2010 and 2015. The report concludes that the overall effect of strict net neutrality for 2011 alone could be $7 billion or 70,000 jobs.

It is important to note, that these projections are based on data from Stratecast's clients and many values in the study have been excised due to non-disclosure agreements.

The argument that net neutrality discourages investment is contested by a 2009 Free Press report, *Finding the Bottom Line: The Truth About Network Neutrality and Investment.* The report argues that investment in the telecom sector is driven far more by other factors than fear of regulation and notes that net neutrality has not had a serious effect on investment in the past.

> ''At the end of 2006, AT&T, as a condition of its acquisition of BellSouth, was required by the [Federal Communications Commission] FCC to operate a neutral network for two years. During this period, while operating under network neutrality rules, AT&T's overall gross investment increased by $1.8 billion -- more than any other ISP in America.''

The report further notes that opposition to net neutrality is not universal among US telecom companies, with new wireless operators such as Clearwire and Cellular South supporting net neutrality, while investing heavily in infrastructure. The report claims that this demonstrates opposition to net neutrality by major telecoms is rooted in a fear of competition rather a fear of harming investment.

> ''During the first half of 2009, Clearwire's capital expenditures were nearly 300% of revenues. This stands in contrast to the investment levels of the most vocal anti-network neutrality ISPs, whose relative investments during the first half of the year were in the mid-to-low teens.''

In a 2010 paper entitled *Free to Invest: The Economic Benefits of Preserving Net Neutrality,* published by the Institute for Policy Integrity, Inimai M. Chettiar and J. Scott Holladay argue that any type of price discrimination that ISPs seek to bring in is an inefficient way of spurring investment and could harm the overall

economic surplus the internet generates.

ISPs are beneficiaries of the 'network effect' whereby networks increase in value as the number of potential connections grows. A good example of this is a telephone network, which becomes more valuable the more people own telephones. Larger ISPs with more subscribers would be able to generate more revenue from price discrimination than smaller players if net neutrality was not enforced, as they would have the existing capital and infrastructure to ensure highly valuable websites and services were available on their networks. Removing net neutrality would therefore reward pre-existing investment, rather than spur investment in new networks. The authors argue it would be far more efficient for the government to guarantee a minimum return on new (rather than pre-existing) network infrastructure, given that most revenue created by price discrimination would be likely to be passed on to shareholders rather than invested in network expansion.

The authors also note that ISPs would likely have difficulty gauging the willingness of content providers to pay for access to their networks, which could result in some providers choosing not to pay at all and this would mean that not all content would be available on every network. The fragmentation of networks that would result from this scenario would also decrease the overall economic value of the internet due to a decreased network effect, as not all content and services would be available on every ISP.

The net neutrality debate in Europe is differed from that in the US, as many EU states have traditionally favoured unbundling of broadband infrastructure as a means of ensuring competition facilitated user access, rather than a strict regulatory environment. Unbundling is when multiple telecommunication providers, including ISPs, are allowed to use the infrastructure (usually telephone lines) between an exchange point and an endpoint (the consumer). A 2009 report by the Technology Policy Institute, *Net Neutrality, Unbundling, and their Effects on International Investment in Next-Generation Networks,* examined the effects of unbundling on the European market. The report claimed that there was insufficient evidence that unbundling would automatically ensure neutral networks but that there was evidence that it would stifle investment in the European market. Noting that states with more unbundling had less investment from incumbent backbone providers in faster fibre networks it concluded that

> ''The more a country relies on unbundled local loops or bitstream unbundling to provide DSL service, the less incumbents and entrants invest in fibre. Similarly, the more platform competition in a country the more investment there is in fibre. In particular, when entrants provide DSL service over their own facilities they also invest more in fiber, and when faced with competition from cable incumbent telcos invest more in fiber.''

Outside of the European and US telecoms markets there has been little investigation of the potential or real economic impact of net neutrality policies. One notable exception to this is Henry L Hu's *The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration,* which looks at the issue in the Chinese context. Hu examines the history of VoIP and p2p in China and explains that these technologies have been impeded because a policy of non-network neutrality is hardwired into the Chinese internet market due to the government's desire to control content. This policy has been directly responsible for the failure of VoIP to develop as a technology in China.

Hu notes that Chinese ISPs routinely slow down or block p2p software in an attempt to conserve bandwidth and draws the conclusion that in China 'the real danger lies in the carriers' capacity of suffocating any innovations such as p2p

that may conflict with ISPs' interest.' Hu notes that 'Chinese ISPs have been the dependent rather than neutral regulatory intermediaries of the government' and are thus required to be non-neutral with regards to outside content the state regards as seditious or destabilising, but also notes that they have blocked or constrained data on purely commercial grounds.

As Hu notes, back in 1997, the Chen brothers in Fu Zhou used net2-phone software to provide overseas calls at much cheaper rates than the state telephone monopoly. At the insistence of the local bureau of telecommunications, the police arrested them and confiscated their assets. The brothers sued the police. Although the case was dismissed on procedural grounds, the court ruled VoIP is a computer information service and not telephony.

Despite this the Ministry of Information Industry (MII) did not accept the decision and ruled VoIP was an exception to standard information services and thus prohibited for 'non-official parties.' Though the MII later liberalised the market somewhat, Hu notes that

> ''[O]nly the five state-owned telecommunication carriers are qualified to obtain such licenses. The MII also restricted the localities for VoIP experiment to only a few cities. The process of VoIP experiment is long and slow due to such restrictions, and VoIP has yet to grow to a mature industry in China after a decade. Meanwhile, private capital is never allowed to invest in VoIP.''

NOTES

3. 'The four principles are that in broadband providing broadband services: 1) consumers are entitled to access the lawful Internet content of their choice. 2) consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement. 3) consumers are entitled to connect their choice of legal devices that do not harm the network; 4) consumers are entitles to competition among network providers, application and service providers, and content providers.

BLOCKING AND FILTERING

THE ARGUMENTS

Outside of human rights-based arguments against censorship, there are serious economic issues to be taken into account when blocking and filtering content. Opponents of blocking and filtering argue that it is expensive to implement these systems, as they can have high investment and operating costs, that they can slow down broadband speed and that they can accidentally restrict access to legitimate content and sites, which can have severe economic consequences for the sites owners.

SUPPORTING STUDIES AND LITERATURE

Research into the effect of censorship and filtering on a state's economy has tended to focus on two states – China and Australia.

China

The true economic effects of China's great firewall are hard to accurately measure. A 2013 article by Beibei Boa, *How Internet Censorship Is Curbing Innovation in China*, reported that one Chinese entrepreneur estimated that bypassing the firewall using a proxy in order to access foreign sites decreased his company's productivity by 10%. The article argued that spread across the country's 10,000 start-ups, such a decrease in productivity could be a huge drain on the nation's economy. In a 2013 survey by the American Chamber of Commerce in the People's Republic of China, *China Business Climate Survey Report* respondents reported that their ability to conduct business normally was increasingly affected by China's internet censorship. While in 2012, 7% of respondents claimed censorship negatively impacted their business and 41% said it 'somewhat negatively' impacted their business, compared to 50% who reported no impact, in 2013, 16% claimed online censorship negatively impacted their business and 39% reported 'somewhat negatively' being impacted, compared to 44% who reported no impact.

Australia

In 2008, the Australian Labor Party government proposed implementing mandatory ISP filtering for illegal content. The move was contested by a large portion of Australian civil society, who feared both the potential for creeping censorship and that filtering at the ISP level would negatively affect the speed of the country's broadband. An article by the Australian news portal Inquisitr entitled The Economic Costs of Internet Censorship in Australia, drawing on the results of an Australian Communications and Media Authority report noted that Australia already has some of the slowest broadband connections in the developed world, and that a further slowing down of the nation's broadband would 'mean quite simply that it takes longer to do business, and that has a negative effect on productivity.'

Again drawing on the ACMA report the Inquisitr noted 'it has been suggested that the filters with the lowest success rate are the quickest, so a proper implementation of a censorship regime would likely, at best cause a 20% drop in internet speeds, but likely significantly higher again.' The article argued that even an increase in AUS $10 a month per customer to cover the administration costs of running such a system would cost AUS $867.6 million a year based on

the number of broadband subscribers in June 2008.

The 2008 report the Inquistr drew on, C*losed Environment Testing of ISP-level Content Filtering r*eported the findings of laboratory tests on six web-filtering systems for efficacy and effect on speed. Their report on the tests found that the six systems caused performance degradation ranging from 2% for one product, 22% to 33% for three products and in excess of 75% for two products.

An essay by Karina Travaglione in 2009 for the Mannkal Economic Education Foundation, *Internet Censorship in Australia – A 'Clean-feed'* noted that a 2004 government-commissioned report found that installation of a mandatory ISP filtering system would cost 'around AUS $45 million as well as ongoing costs of greater than AUS $33million per year in administrative costs for filtering by the providers'.

The report noted that the Labor government had budgeted only $44 million over four years for installation and nothing for administrative costs, meaning that in addition to paying more in taxation, the cost of the system would have to be born by consumers.

ONLINE SURVEILLANCE

THE ARGUMENTS

While the ability of states to intercept, store, access and analyse individuals' private data is of course an important issue for human rights advocates, the economic impact of online surveillance is also a serious concern. The most common economic concern about the prevalence of online surveillance is that it undermines trust in confidentiality and data protection, thus harming the ability of actors to carry out business online. If the security of sensitive information cannot be secured online, it decreases the usefulness of the internet as a medium for carrying out economic activity. Both individuals and organisations may be less likely to trust intermediaries with private or sensitive information, not only decreasing the overall profits of intermediaries but also preventing these same individuals and organisations from taking advantage of efficiencies in communication and data storage.

The non-transparent nature of online surveillance also diminishes trust between states, who fear other states (including friendly ones) could be engaging in espionage against them. This limits the ability of companies from one state (who may be forced to hand over data to their government's security services) to do business in another, decreasing both trade and foreign investment. As Jason Healey of the Atlantic Council argues in relation to US spying revelations, 'People aren't going to trust the U.S. and U.S. companies as much… you're going to see national boundaries begin in cyberspace.'

The concern that 'national boundaries' will reappear in cyberspace has implications not only for the ability of internet companies to do business in different jurisdictions, it has consequences for the entire internet ecosystem itself. As Gene Kimmelman, President and CEO of Public Knowledge, puts it, 'The private sector is very worried about [the NSA revelations] because it messes with what might be [the] most economic way to route message flows and traffic, if you're forced to have equipment in a certain country, by law, it might add significant expense to an operation.' [4]

Some have gone as far as to argue that fears of online surveillance by states could lead to a breakdown of the internet itself in favour of numerous nationally-based, smaller, competing internets, isolated and walled off from each other. Such a 'balkanised' system would undermine one of the central economic benefits of the internet: the ability to overcome borders and facilitate communication and trade on a worldwide scale. Many viewed Brazilian President Dilma Rouseff's plan to create an encrypted email service based on the state postal service and force major internet companies to store all data on Brazilian customers on servers based on Brazilian soil as another step towards a balkanised internet. Comparing such an internet to Europe's non-standardised and non-interoperable system of rail networks, Sascha Meinrath of the Open Technology Institute noted in an article entitled *We Can't Let the Internet Become Balkanised* that in a balkanised internet,

> ''Netizens would fall under a complex array of different jurisdictions imposing conflicting mandates and conferring conflicting rights. And much as different signalling hampers the movement of people and the trade of physical goods, an Internet within such a complex jurisdictional structure would certainly hamper modern economic

activity.''

SUPPORTING STUDIES AND LITERATURE

Discussion of the economic effects of surveillance on the national level has tended to focus on the US. Little investigation has been done on how internet surveillance systems such as Russia's 'SORM-3' affect their states' economies. This is probably due to the outsized role of US-based multinationals in the online economy and the large proportion of internet architecture based on US territory, which gives the US government an advantage over others in online surveillance and espionage. Nevertheless, at least one estimate has tried to look at the financial fallout from increased surveillance concerns.

Attempts to quantify the economic fallout from Snowden's revelations of mass surveillance seem to indicate that widespread government surveillance negatively impacts the ability of companies from that country to do business abroad. A July 2013 survey from the Cloud Security Alliance entitled *Government Access to Information Survey Results*, polled 426 individuals (234 respondents identified themselves as responding from the US, and 222 from the rest of world) working in security in the cloud computing industry on their opinions on what they called the 'Snowden incident.' 56% of non-US respondents claimed the revelations made them less likely to use US-based cloud providers, with 10% claiming they had actually cancelled a project to use US-based cloud providers due to the revelations. Similarly 36% of US respondents claimed the revelations made it more difficult for them to conduct business outside the US.

Other studies have also attempted to estimate the economic effects of online surveillance on a more global scale. Extrapolating from the Cloud Security Alliance survey, The Information Technology and Innovation Foundation (ITIF) issued a report, *How Much Will PRISM Cost the U.S. Cloud Computing Industry?* The report looked at the Cloud Computing Industry, and noted that, according to a report by Gartner, the global cloud computing market will be a $207 billion industry by 2016. The report notes that cloud computing is a rapidly expanding industry and suggests

> ''The impact of PRISM on U.S companies may be particularly acute because cloud computing is a rapidly growing industry. This means that cloud computing vendors not only have to retain existing customers, they must actively recruit new customers to retain market share. Global spending on cloud computing is expected to grow by as much as 100% between 2012 and 2016, whereas the global IT market will only grow by 3%.''

The report goes on to note that a loss of 10% in foreign markets to European and Asian competitors, which the report considers to be at the low end of what can be expected, would translate into a loss of $21.5 billion for US companies over the next three years. A loss of 20% in foreign markets, which would be at the high end of what could be expected, would translate into a loss of $35.0 billion by 2016.

James Staten, an analyst at Forrester, a data security company, noted that the economic effects of increased concern about online surveillance stemming from the Snowden revelations both in America and worldwide were likely to be bigger than ITIF predicted. Staten noted 'US customers would also bypass US cloud providers for their international and overseas business - costing these cloud providers up to 20% of this business as well' and that 'non-US cloud providers will lose as much as 20% of their available overseas and domestic opportunities' as revelations of surveillance programmes in their own states become common.

States may insist data on their citizens be held on servers in their own territory. This decline in investment and lack of trust between actors in different jurisdictions, combined with increased administrative costs and inefficiencies from having to use separate service providers in different states with different legal requirements and regulatory frameworks on data protection could add an extra $10 billion to the overall losses for US cloud storage providers.

> ''Short term, a greater understanding of this surveillance picture could have a chilling effect on all hosting and outsourcing services (not just cloud computing) in many countries. If it is to be believed, as ITIF estimates, that half the cloud market will be fulfilled by non-US providers, then assuming this factor has just as much impact as the PRISM leak will have on US providers, then non-US cloud providers would take a hit of another $35 billion by 2016.''

The report notes that the net loss of increased concern over surveillance could come to net loss of $180 billion by 2016. The report does note though that this is by no means certain and that the economic benefits of increased efficiencies from cloud providers, hosting and outsourcing may cause governments to reconsider such economically devastating policies.

NOTES

4. http://www.bloomberg.com/news/2013-11-26/nsa-spying-risks-35-billion-in-u-s-technology-sales.html

INTERMEDIARY LIABILITY

THE ARGUMENTS

In most of the developed world, intermediary liability for user-generated data is usually limited by law, provided certain criteria are ensured. As the OECD report notes.

> ''The limited liability component of the Digital Millennium Copyright Act (DMCA) creates a conditional safe harbour from copyright liability for online service providers for functions of transmission and routing ('mere conduit' functions), caching, storing, and 'information location tools' including online directories and providing links to third party materials alleged to infringe the copyrights of others. Similar principles on the liability of online intermediaries also exist in Australian copyright law.''

Since they facilitate the overwhelming majority of online commercial activity in different ways, internet intermediaries are clearly of vital importance economically. Despite this, little empirical research has been conducted into the economic impact of different liability regimes.

SUPPORTING STUDIES AND LITERATURE

The Center for Technology and Democracy (CDT) in a 2010 report, *Intermediary Liability: Protecting Internet Platforms for Expression and Innovation* argues that intermediary liability for user-generated data has an overall negative economic effect.

> ''Without protection from liability, companies are less likely to develop new ICT products and services. The threat of liability will also tend to close the market to start-ups, which are often unable to afford expensive compliance staffs. The threat of liability may thereby entrench existing market players, who will be less driven to innovate or improve upon existing business models. Many businesses may simply choose to operate only in countries where ICT intermediaries are granted broad liability protections, resulting in less foreign direct investment in those countries that do not grant such protections.''

The report looks at the liability regimes in the US, the EU and China but does not provide any data on the economic impact of these regimes. Drawing from a report by the Institute for Prospective Technological Studies, CDT suggests that the comparative weakness of the European Web 2.0 sector may stem from, among other things, the EU's more onerous liability regime for intermediaries. Although web 2.0 applications are almost as widely used in the EU as in the US, 'about two-thirds of major Web 2.0 applications are provided by U.S. companies, with Europe lagging far behind in revenue and innovation indicators.' Europe for its part, provides only about 10% of Web 2.0 applications.

Outside of the developed world, intermediary liability is seldom clearly defined by legislation. The Dalberg Group's report, *Open for Business*, examined Thailand as a case study and argued that the country's vague 2007 'Act on Computer Crime' led to local start-ups and businesses having to pay large costs to avoid

litigation for third party content. The report noted that the user-moderated discussion site, 212cafe.com had to close due to concerns about liability and that pantip.com, a consumer reviews site had to devote a large amount of time and effort to deleting reviews (many of which the owner considered legitimate) due to concerns about litigation. Dalberg quoted Mike Godwin, Senior Policy Advisor to the Global Internet Policy Project at Internews as saying, 'If I were a Thai entrepreneur and wanted to create an Internet application for Thailand right now, the first thing I would do is move to Singapore.'

The report noted that even when protections for intermediaries from liability are enshrined in legislation, a state's legal system can still cause problems if this legislation is not widely understood. Looking at the highly popular user-content driven site Eksi Sözlük, the report notes that

> ''Despite legal protections exempting the site from liability for third-party content, founder and CEO Sedat Kapanoglu spends at least one day a month in court defending the site and educating prosecutors and judges about the protections afforded to him by law.''

A 2012 Association for Progressive Communications paper, The Liability of Internet Intermediaries in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain examined the issue in African context. The report noted that intermediary liability and 'safe harbour' provisions are addressed by law only in South Africa and Uganda. The report found that

> ''While there is some protection for intermediaries from liability in South Africa and Uganda, intermediaries in all countries in the study operate under an uncertain environment, and could be exposed to undue liability that could hamper the development of the information society and economy.''

CONCLUSIONS: STATE OF EVIDENCE

Although it is clear that there is a large amount of theoretical arguments that internet policies that respect human rights bring tangible economic benefits, as well as a body of empirical evidence that this is true in certain circumstances, much of the research and analysis on these issues has suffered from several limitations.

Research has predominantly focused on the large and relatively developed economies of the G20. This focus has also meant that research has tended to ignore the economic impact of policies in the global South. Research into the economic effects of internet policies has tended not to focus on Latin America or Africa though there is reason to believe this situation will change as internet penetration and use increase in these markets and the importance of internet governance increases in these states' policy circles. Legal initiatives like Brazil's Marco Civil, or Chile's Bulletin 4915, which guarantees net neutrality, show this has already taken place in recent years.

Research into the economic effects of net neutrality has been heavily skewed towards the US market, which is a particular model whose lessons may not be easily extrapolated to other markets, even those of other advanced economies such as Europe. Research into the economic impact of online surveillance has also been heavily centred on the economic effects of online surveillance by the United States. While this is clearly a reaction to the outsized role US-based intermediaries play in the internet, and the centrality of the US to the infrastructure of the internet, the economic impact of surveillance in other states has not been quantified to anything near the same extent. Similarly, while the effects of online blocking and filtering have been examined in Australia and China, these countries do not necessarily constitute a useful model to extrapolate from. China's vast domestic market means it is less economically dependent on foreign intermediaries and Australia's geographic isolation and slow internet speeds may make it more vulnerable to a drop in broadband speed than other markets.

Economic research has also tended to focus on certain issues rather than others. Net neutrality has attracted the lion's share of attention. Online surveillance and filtering and blocking have attracted comparatively less interest and research though some empirical evidence that filtering and blocking and broad online surveillance have a negative economic effect has been established. The impact of intermediary liability regimes, unfortunately, has not attracted much concrete investigation. Possibly because the debate is primarily about how best to enshrine protections in law and establish where liability should indeed arise.

In order to consolidate the body of evidence available on the economic effects of a human rights-based internet, more research needs to be carried out on the economic effects of net neutrality, intermediary liability, filtering and blocking, and online surveillance on different states, including those in the global South. Comparative case studies should be carried out in order to better understand if the findings are applicable across different markets and states. The relationship (if any) between foreign direct investment in the internet industry and the extent to which a state respects human rights online could be a fruitful line of inquiry for further research. Indicators such as number of start-ups and the development of internet exchange points within states could also be useful in gauging how a human rights-based approach to internet governance affects a state's economy.

The future of the internet is being decided right now and the type of internet we end up with will depend in major part on the decisions of policymakers across the world. If we wish to convince policymakers of the economic benefits of a human rights-based internet, we will need to make sure our arguments and our evidence are more detailed, more universal and as compelling as possible.

ANNEX - KEY FINDINGS FROM SUPPORTING STUDIES AND LITERATURE

INTERNET USAGE AND INTERNET PENETRATION

Increased internet usage, and broadband penetration is positively correlated with economic benefits.

- Every 10 percentage point increase in broadband penetration increases GDP by 1%.
- Doubling the broadband speed for an economy increases GDP by 0.3%.
- The internet is also responsible for an increasing share of many states' GDPs.
- In 2010 the internet contributed to 4.3% of the economies of the G20's developed states but only 3.6% to the economies of its developing markets, by 2016 the figures were expected to be 5.5% and 4.9% respectively.
- The internet accounted for 10% of GDP growth over the past 15 years in 13 developed economies but that over the past five years, the internet's contribution to GDP growth in the countries doubled to 21%.
- A study sponsored by several American telecoms argued that between 2010-2015, strict net neutrality would.
- Cost customers an extra $10 to $55 per month on top of their existing average payment of $30.
- Cost broadband operators an extra $20 billion to $40 billion per year in increased costs of increasing network capacity, rather than spending this money on extending their broadband networks.
- Cost the US economy $20 billion to $100 billion.
- Cost US economy $7 billion or 70,000 jobs in 2011 alone.

A Free Press report countered these claims noting

- Investment in expanding broadband networks does not seem to be correlated with net neutrality.
- ATT invested more in expanding its network than any other ISP in a period during which it was forced to operate a strict neutral network to comply with an FCC ruling.
- Clearwire, an ISP that supports net neutrality, spent 300% its income for 2009 on extending its broadband network.

NETWORK NEUTRALITY

Net neutrality in Europe

- Is not guaranteed by unbundling.
- Bundling is correlated with a lack of investment in broadband fibre networks.

A lack of net neutrality in China

- Has led to blocking of services that compete with ISPs economic interests, like p2p.
- Has led to an extremely underdeveloped VoIP service market.

African markets are lacking in clearly defined intermediary liability laws, which may impede investment.

27

BLOCKING AND FILTERING

Online filtering and blocking in China

- Has been linked to a loss of 10% productivity for Chinese start-ups.

In 2013 16% of Americans doing business in China claim online censorship has negatively affected their ability to do business and 39% claim it has somewhat negatively affected their ability to do business, compared to 7% and 41% respectively in 2012.

Online filtering and blocking in Australia

- Could cost broadband costumers an extra AUS $10 per month.
- Could cost AUS $45 million in initial investment and AUS $33 million in yearly operating costs.
- Could cause a drop of 20% in broadband speeds.
- Australia's average broadband speeds are already some of the lowest in the developed world.

INTERMEDIARY LIABILITY

Recent revelations of extensive state surveillance have negatively impacted confidence in intermediaries ability to protect their costumers data and this has affected the market.

- 56% of non-US respondents to a survey on the PRISM revelations said they are now less likely to use US-based cloud providers.
- Similarly, 36% of US-based cloud computer providers surveyed claimed the revelations make it difficult to do business outside the US.
- Loss of confidence in US companies could cost them $21.5 billion to $35 billion by 2016.

The net result of increased concern over online government surveillance could cost the world economy $180 billion by 2016.

BIBLIOGRAPHY

Beibei Boa, *How Internet Censorship Is Curbing Innovation in China* (The Atlantic, 22 April 2013)

Daniel Castro, *How Much Will PRISM Cost the U.S. Cloud Computing Industry?* (The Information Technology and Innovation Foundation, August 2013)

Inimai M. Chettiar, J. Scott Holladay, *Free to Invest: The Economic Benefits of Preserving Net Neutrality,* (Institute for Policy Integrity, New York University School of Law, January 2010)

China Business Climate Survey Report (American Chamber of Commerce in the People's Republic of China, 2013)

Closed Environment Testing of ISP-level Content Filtering: Report to the Minister for Broadband, Communications and the Digital Economy, (Australian Communications and Media Authority, June 2008)

Alex Comninos, *The liability of Internet Intermediaries in Nigeria, Kenya, South Africa and Uganda: An Uncertain Terrain (*Association for Progressive Communications, October 2012)

David Dean, Sebastian Digrande, Dominic Field, Andreas Lundmark, James O'Day, John Pineda, Paul Zwillenberg, *The $4.2 Trillion Opportunity: The Internet Economy in the G20* (The Boston Consulting Group, March 2012)

The Economic Costs of Internet Censorship in Australia (The Inquisitor, February 5, 2009)

Frank le Rue, *Report of the Special Rapporteur on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet* (United Nations General Assembly A/HRC/17/27, 16 May 2011)

Nicole Gaouette, *NSA Spying Risks $35 Billion in U.S. Technology Sales* (Bloomberg, 26 November 2013)

Arthur Goldstuck, *Internet Matters: The Quiet Engine of the South African Economy* (World Wide Worx 2012)

Government Access to Information Survey Results (Cloud Security Alliance, July 2013)

Henry L. Hu, *The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration* (The China Quarterly 205, 2011)

Intermediary Liability: Protecting Internet Platforms for Expression and Innovation (The Center for Technology and Democracy, April 2010)

Carl Kalapesi, Sarah Willersdorf, Paul Zwillenberg, *The Connected Kingdom, How the Internet is Transforming the UK Economy* (The Boston Consulting Group, October 2010)

Sascha Meinrath, *We Can't Let the Internet Become Balkanised* (Slate, 14 October 2013)

Net Neutrality: Impact on the Consumer and Economic Growth (Stratecast, May 2010)

Open for Business? The Economic Impact of Internet Openness (Dalberg, March 2014)

Gernot Pehnelt, *The Economics of Net Neutrality Revisited* (Friedrich-Schiller-University Jena, Max-Planck-Institute of Economics, 27 October 2008)

Matthieu Pélissié du Rausas, James Manyika, Eric Hazan, Jacques Bughin, Michael Chui, Rémi Said, *Internet Matters: The Net's Sweeping Impact on Growth, Jobs and Prosperity* (McKinsey Global Institute, May 2011)

Karine Perset, *The Economic and Social Role of Internet Intermediaries* (OECD April 2010)

James Staten's Blog, *The Cost of PRISM Will Be Larger Than the ITIF predicts*. (Accessed 14 August 2014, http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects)

Karina Travaglione, *Internet Censorship in Australia – A 'Clean-feed'* (Mannkal Economic Education Foundation, July 2009)

The 3 Billion Question: Does the Internet accelerate Economic Growth (Markle Foundation, July 2012)

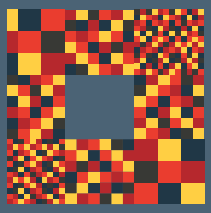
S. Derek Turner, *Finding the Bottom Line: The Truth About Network Neutrality and Investment.* (Free Press, October 2009)

UN General Assembly, Universal Declaration of Human Rights (10 December 1948)

UN General Assembly, International Covenant on Civil and Political Rights (16 December 1966)

J Scott Wallsten and Stephanie Hausladen, *Net Neutrality, Unbundling, and their Effects on International Investment in Next-Generation Networks* (Technology Policy Institute, March 2009)

Paul Zwillenberg, Dominic Field, David Dean, T*he Connected World: Greasing the Wheels of the Internet Economy* (Boston Consulting Group, January 2014)



GLOBAL PARTNERS DIGITAL

GLOBAL PARTNERS DIGITAL
Development House
56–64 Leonard Street
London EC2A 4LT
+44 (0)20 7549 0336
gp-digital.org